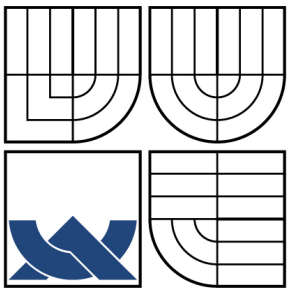
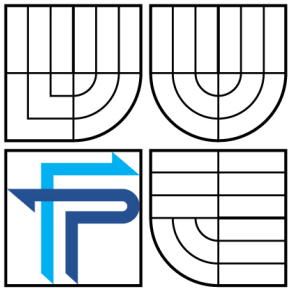


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ZABEZPEČENÍ A OCHRANA DAT VE FIRMĚ

DATA SECURITY AND DATA PROTECTION IN THE FIRM

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — LUDMILA NAVRÁTILOVÁ

AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.

SUPERVISOR

BRNO 2007

Vysoká škola: Vysoké učení technické v Brně | Akademický rok: 2006/2007

Fakulta: podnikatelská | Ústav: informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ludmila Navrátilová

6209R021 - Manažerská informatika

Ředitel ústavu v souladu se zákonem č. 111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů Vám zadává bakalářskou práci s názvem:

Zabezpečení a ochrana dat ve firmě

Data Security and Data Protection in the Firm

Pokyny pro vypracování:

Úvod
Cíl práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr

Rozsah grafických prací: dle potřeby

Rozsah původní zprávy: cca 40 stran

Seznam odborné literatury:

DOSEDĚL, T.: Počítačová ochrana a ochrana dat. 1. vyd. Brno: Computer Press. 2004. 190 s. ISBN: 80-251-0106-1
GÁLA, L., POUR, J., TOMAN, P.: Podniková informatika. 1. vyd. Praha: Grada. 2006. 484 s. ISBN: 80-247-1278-4
LEBER, J.: Windows NT. Zálohování a obnova dat. 1. vyd. Praha: Computer Press. 1998. 282 s. ISBN: 80-7226-123-1
RODRYČOVÁ, D., STAŠA, P.: Bezpečnost informací jako podmínka prosperity firmy. 1. vyd. Praha: Grada. 2002. 144 s. ISBN: 80-7169-144-5
norma ČSN BS 7799-2

Vedoucí bakalářské práce: Ing. Viktor Ondrák, Ph.D.

Datum zahájení bakalářské práce: 31. října 2006

Datum odevzdání bakalářské práce: 31. května 2007

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta podnikatelská
L. S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

Doc. Ing. Miloš Koch, CSc.
Děkan

V Brně dne: 16. února 2007

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Ludmila Navrátilová

Bytem: Struha 789, 517 54 Vamberk

Narozen/a (datum a místo): 8. června 1985, Opočno

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta podnikatelská

se sídlem Kolejní 2906/4, 612 00 Brno

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

Ing. Jiří Kříž, Ph. D., ředitel Ústavu informatiky

(dále jen „nabyvatel“)

Čl. 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - ☐ disertační práce
   - ☐ diplomová práce
   - ☒ bakalářská práce
   - ☐ jiná práce, jejíž druh je specifikován jako .....

   (dále jen VŠKP nebo dílo)

Název VŠKP:	***Zabezpečení a ochrana dat ve firmě***
Vedoucí/ školitel VŠKP:	Ing. Viktor Ondrák, Ph. D.
Ústav:	Ústav informatiky
Datum obhajoby VŠKP:	červen 2007

VŠKP odevzdal autor nabyvateli v*:

- ☒ tištěné formě – počet exemplářů: 1
- ☒ elektronické formě – počet exemplářů: 1

* hodící se zaškrtněte

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - ☒ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.

Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.

2. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
3. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: …….

....

Nabyvatel Autor

Abstrakt

Tato práce se zabývá zabezpečením a ochranou dat ve velké společnosti. Popisuje současný stav ve firmě. Na základě zjištěných skutečností obsahuje možné návrhy bezpečnosti informačního systému firmy a zálohování.

Abstract

This work deals with the data security and protection in a big company. It describes the current status in the company. Based on findings it provides possible proposals on data security of information system and back up.

Klíčová slova

zabezpečení dat, bezpečnost informačního systému, bezpečnostní normy, zálohování, povědomí zaměstnanců o bezpečnosti

Key words

data security, security of information system, security standards, backup, staff awareness about security

Bibliografická citace mé práce

NAVRÁTILOVÁ, L. *Zabezpečení a ochrana dat ve firmě*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2007. 55 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracovala jsem ji samostatně.

Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušila autorská práva (ve smyslu zákona č. 121/2000 Sb. o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31. května 2007 .....

podpis

Poděkování

Tímto bych chtěla poděkovat všem, kteří mi poskytli informace, cenné rady a praktická poučení, zejména panu Ing. Viktoru Ondráku, Ph. D., vedoucímu mé práce.

OBSAH

Úvod

V současné době se firmy stále více opírají o informační a komunikační technologie, produkují, zpracovávají a ukládají čím dál větší množství pro ně životně důležitých dat. S tím, jak roste množství a důležitost dat, roste i jejich hodnota – a s ní i riziko odcizení, poškození či úplné ztráty. Toto nebezpečí si firmy většinou velice dobře uvědomují, a proto investují do oblasti zabezpečení, ukládání a zálohování dat stále více prostředků.

Nejde jen o hledisko zaměřené pouze na technologie, ale jedná se o prioritní záležitost celého podniku. Z toho důvodu čelí pracovníci zodpovědní za podnikové informační systémy a jejich týmy závažným problémům. Jejich cílem je ukázat ostatním zaměstnancům, v čem spočívá hodnota komplexního zabezpečení informačních systémů a implementovat řešení, která takové zabezpečení poskytnou.

Efektivní ochrana informací vyžaduje především detailní znalost existujících slabin informačního systému. Pouze znalost potenciálních bezpečnostních rizik umožňuje zavést efektivní a výkonná ochranná opatření. Cílem budování bezpečnosti IS/ICT je vytvoření uceleného systému, který podporuje efektivní styl řízení a správy této oblasti, včetně precizního stanovení hierarchie odpovědností, povinností a práv jednotlivých subjektů, kteří do prostředí IS přistupují.

Cíl práce

Cílem práce je optimalizovat bezpečnostní prvky v konkrétní firmě. Na základě poznatků z analýzy současného stavu zabezpečení firmy a teoretických východisek se pokusím nastínit možné návrhy řešení zjištěných problémů bezpečnosti firmy.

1 Analýza firmy

V této kapitole se budu zabývat analytickou částí firmy, kde představím firmu jako celek, dále její stav využívaných informačních systémů a technologií, analýzu zabezpečení, kterou firma v současné době aplikuje, poté procesy zálohování, jenž zvyšují zabezpečení dat a poslední součástí samotné analýzy je obnova systému.

Závěrem této analýzy je přehled nedostatků firmy, ve kterém jsem se pokusila vystihnout stěžejní problémy bezpečnosti firmy.

1.1 Charakteristika firmy

1.1.1 Základní údaje o firmě

Obchodní jméno společnosti:	***Federal-Mogul Friction Products, a. s.***
Sídlo společnosti:	Jirchářská 233, 517 41 Kostelec nad Orlicí
Identifikační číslo společnosti:	455 34 144, registrováno v Obchodním rejstříku vedeného Krajským soudem v Hradci Králové oddíl B, vložka 561

Jedná se o velký podnik, v kterém je v současné době zaměstnáno asi 850 pracovníků. Firma je orientována na automobilový průmysl.

1.1.2 Předmět podnikání

Hlavním předmětem podnikání společnosti je vývoj, výroba a prodej brzdového a spojkového obložení, třecích segmentů kotoučových brzd, pásového obložení brzd, speciálních výrobků z třecích materiálů, ucpávkového provazcového těsniva tkaných pásů suchých a impregnovaných. Tento vývoj a výroba probíhá s vyloučením použití azbestu v souladu s příslušnými mezinárodními úmluvami přijatými vládou České republiky.

Základní strategie společnosti ve výrobě třecích materiálů je orientace na výrobu brzdového obložení pro osobní a nákladní vozidla a diskových brzd pro osobní vozidla.

1.1.3 Vývoj společnosti

Akciová společnost Ferodo, a. s. byla založena 9. dubna 1992 podle § 172 Obchodního zákoníku č. 513/91 Sb. a jediným akcionářem je společnosti T&N Limited se sídlem v Manchesteru.

Dne 1. června 1992 vložil Fond národního majetku do společnosti majetek společnosti Osinek, a. s. a získal 45% podíl. K 1. říjnu 1997 Fond národního majetku odprodal svůj podíl společnosti T&N Limited, která se tak stala jediným akcionářem.

Dne 6. března 1998 byla společnost T&N Limited převzata společností Federal-Mogul Corporation, Southfield, USA. K 1. říjnu 1998 byl proveden výmaz původního obchodního jména Ferodo, a. s. z Obchodního rejstříku a zapsáno nové obchodní jméno Federal-Mogul Friction Products, a. s.

1.1.4 Právní forma společnosti

Firma je akciovou společností, proto je povinna tvořit rezervní fond v roce, kdy poprvé dosáhne zisku, a to ve výši 20 % čistého zisku, ne však více než 10 % základního kapitálu.

Základní kapitál:	10 000 000,- Kč
Akcie:	10 000 ks akcie na jméno ve jmenovité hodnotě 1 000,- Kč
Zákonný rezervní fond:	2 000 000,- Kč

1.1.5 Zákazníci firmy

Firma dodává své produkty jak přímo prvovýrobcům brzdových systémů, tak i na trh náhradních dílů. Společnost exportuje více než 90 % své produkce. Nejvíce

exportů je v rámci skupiny třecích materiálů společnosti Federal-Mogul, a to do jejich ostatních výrobních podniků a distribučních center, tzv. aftermarketů.

Konečnými zákazníky a příjemci výrobků vyrobených v Kostelci nad Orlicí jsou KNOTT, RABA, IVECO, SMB, SAE, Daimler Chrysler a další. Mimo skupinu společnost prodává nejvíce svých výrobků zákazníkům jako je IVECO, BOSCH, WABCO, VOLKSWAGEN, ISUZU, RENAULT, VOLVO a FTE.

1.1.6 Organizační struktura

Společnost má následující organizační strukturu:
viz *Příloha 1 – Organizační struktura společnosti*

1.1.7 Vztahy společnosti k vyšší organizační jednotce

Mateřskou společností je T&N Limited, Manchester Internationl Office Centre, Styal Road, Manchester M22 5TN, United Kingdom, mateřskou společností celé skupiny je Federal-Mogul Corporation, Michigan, USA. Společnost je součástí jejího konsolidačního celku.

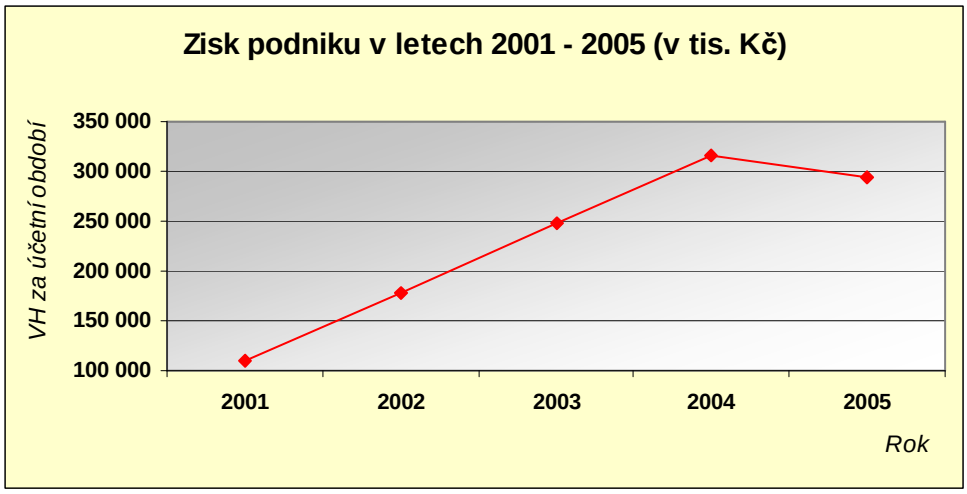
Od mateřské společnosti přebírá Federal-Mogul jednotlivé strategie a plány, kterými se musí řídit.

1.1.8 Ekonomický ukazatel firmy

Zisk

	2001	2002	2003	2004	2005
VH za účetní období	110 595	177 372	248 808	315 717	293 328

Tabulka 1: Zisk podniku v letech 2001 – 2005 (v tis. Kč)



Graf 1: Zisk podniku v letech 2001 – 2005 (v tis. Kč)

Zisk podniku má rostoucí charakter rok od roku kromě roku 2005, kde jeho výše klesla o 22 389 tis. Kč. To mohlo být způsobeno nárůstem mzdových nákladů, nákladů na sociální zabezpečení a zdravotní pojištění a zvýšenou spotřebou energie.

1.2 Současný stav informačních technologií využívaných ve firmě

1.2.1 Stav výpočetní techniky a operačních systémů

Od roku 2006 firma postupně přechází na používání hardwaru od společnosti ***Dell***, což patří mezi již zmiňované strategie mateřské společnosti. Dell by měl být v budoucnu pro celý Federal-Mogul globálním dodavatelem veškerého hardwarového vybavení.

Ze softwarových možností firma využívá ***Lotus Notes/Domino*** od ***IBM***. Tato technologie je typu klient server a její aplikace je obvykle umístěna na serveru a klient komunikuje s touto aplikací. Přístup k aplikaci je ve Federal-Mogulu nativním protokolem. Nativní komunikační protokol NRPC (Notes Remote Procedure Call) je použit pro komunikaci mezi serverem Domino a klientem Notes a vzájemně mezi

Domino servery. Serverová část se nazývá *IBM Lotus Domino* a klientská část *IBM Lotus Notes*.

Bezpečnost Lotus Notes je založena na existenci tzv. ID souborů. V těchto souborech jsou uloženy certifikáty, digitální podpisy, šifrovací a dešifrovací klíče a další citlivé informace. Lotus Notes/Domino používá RSA (Rivest-Shamir-Adleman) kryptování veřejným klíčem k zajištění čtyř základních úrovní bezpečnosti: ověření totožnosti a oprávnění přístupu (X.509 certifikáty), šifrování zpráv a digitální podpisy. Každý uživatel má svůj jedinečný ID soubor. Díky tomuto ID a architektuře se dají data zabezpečit na mnoha úrovních, které připomínají trychtýř, ve kterém je na každé úrovni menší síto, než na úrovni předchozí.

Novell Evolution je ve firmě osobním informačním manažerem. V Novellu zaměstnanci firmy využívají poštovního klienta, adresář a kalendář. Výhodou tohoto softwaru je inteligentní třídění nevyžádané pošty, šifrování zpráv, filtry, podpora pro web kalendář, podpora pro Microsoft Exchange 2002/2003 a Novell GroupWise.

Do dvou až tří let chce Federal-Mogul přejít z Lotus Notes a Novell Evolution na aplikace od Microsoftu.

Zaměstnanci společnosti využívají operační systémy Windows a to z poloviny ***Windows 2000*** a ***Windows xp.***

Společnost Dell pro Federal-Mogul zavedla globální podporu informačních systémů ***Client Service Desk*** (Help Desk). Zaměstnanci firmy se na tuto mezinárodní bezplatnou pomoc mohou obracet telefonicky a to 24 hodin denně sedm dní v týdnu. Jedná se o jednotné kontaktní místo v Rumunsku a Indii s úplným rozsahem odpovědností s vícejazyčnou podporou (čeština zde ale není zahrnuta) a ve Federal-Mogulu v Kostelci nad Orlicí funguje od konce dubna 2006.

1.2.2 Softwarová spolupráce komponent v budoucnosti firmy

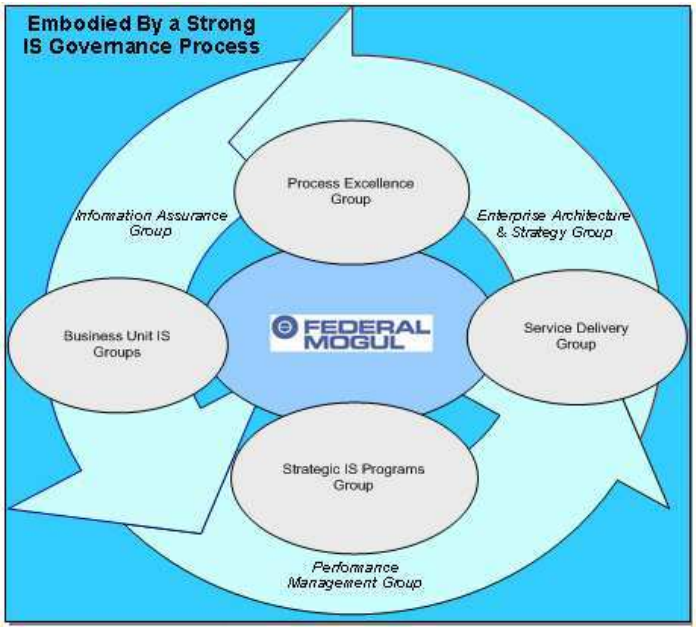
V celé reorganizaci IS a IT chce firma do dvou až tří let přejít na stejný HW a SW. Co se týká SW, tak je to tento:

- Share Point – komunikační nástroj a centrální sklad pro dokumenty.
- Live Communications Server – slouží k okamžitému odesílání zpráv pro sdílení plánů a informací pro okamžité řešení obchodních kontaktů.

- Microsoft Office 2007 – zmodernizovaná sada aplikací MO.
- Live Meeting 2005 – webový konferenční servis, který umožňuje uživateli spolupracovat online s ostatními kolegy, zákazníky, partnery v reálném čase a to buď mezi jednotlivci nebo mezi většími skupinami.

Obrázek 1: Vize globálního řešení IS/IT Federal-Mogulu[1]

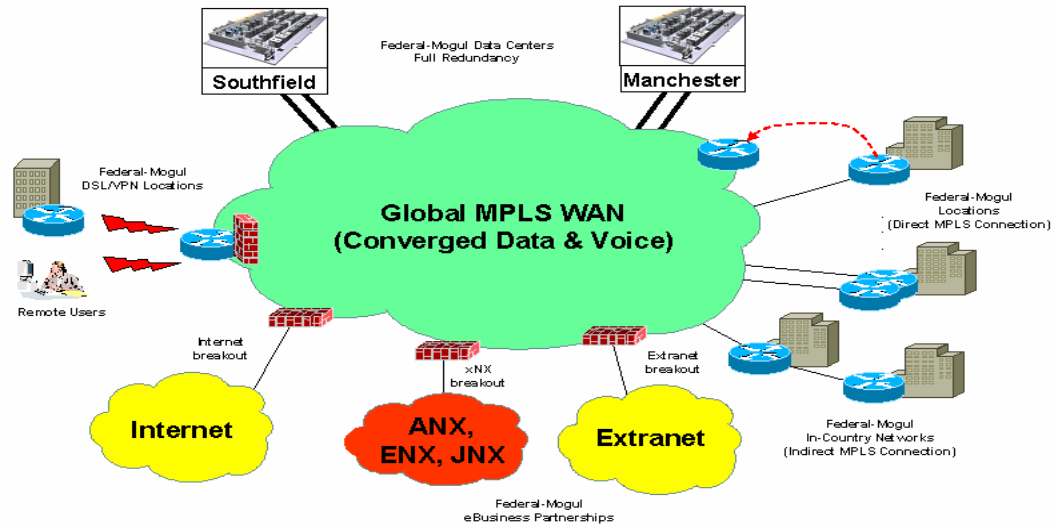
1.2.3 Informační systém a informační toky ve firmě



Obrázek 2: Organizace IS[1]

[1] *Information Systems Service Delivery - Global Infrastructure*. 2006

Celé informační systémy firmy procházejí reorganizací a cílem je sjednotit všechny do jednoho systému. Celý systém by měl být vysoce obchodně orientován a všechny části by měly být spojeny do středu obchodního dění. Cílem IS firmy je, aby byl předvídavý a cílevědomý.



Obrázek 3: Globální síť WAN podporující obchodní procesy[2]

Současný celkový stav IS pro Federal-Mogul

- 185 míst na celém světě
- 16 000 PC

<u>z toho ve Federal-Mogul, a. s. v Kostelci nad Orlicí</u>

- 310 uživatelů
- 220 PC
- 30 notebooků

- MFG/PRO – hlavní informační systém – 175 uživatelů
- Novell – přihlášení k síti – 250 uživatelů
- Internet – 120 uživatelů

[2] *Information Systems Service Delivery - Global Infrastructure*. 2006

Informační systém MFG/PRO

Firma využívá informační systém MFG/PRO, který je plně integrovaný ERP systém pro plánování podnikových zdrojů, implementovatelný po jednotlivých modulech. Tato aplikace se používá pro malosériovou výrobu, výrobu na sklad, konfigurace na zakázku i pro sériovou výrobu.

MFG/PRO pokrývá oblasti: prodeje, nákupu, plánování výroby, výrobu, řízení zásob, řízení jakosti, servis a finance.

Řízení dodavatelských vztahů umožňuje komunikaci se zákazníky a dodavateli prostřednictvím rozvrhů a odvolávek (nikoli objednávek), ve kterých lze dodávané množství rozvrhovat v čase a dosáhnout tak užší spolupráce s partnerem případně až komunikace na úrovni JIT (Just-In-Time).

1.3 Analýza zabezpečení

1.3.1 Správa uživatelů

Správce každého systému musí zajistit pro každého uživatele jedinečné přihlašovací jméno. Sdílení jednoho uživatelského jména mezi více uživateli je nepřípustné, neboť uživatelské jména slouží ke sledování činností uživatelů v jednotlivých systémech. Výjimku z tohoto pravidla může udělit pouze oddělení Information Security v Southfieldu.

Hesla k jednotlivým uživatelským jménům musí být držena v tajnosti a nesmějí být nikde uvedena v psané podobě.

Zaměstnanci však nedodržují všeobecné zásady při tvorbě silných hesel. Přihlašování do systému si snaží mnoha způsoby ulehčit.

1.3.2 Elektronická pošta

Systém elektronické pošty ve Federal-Mogul, a. s. by měl sloužit výhradně k pracovním účelům a neměl by být používán jiným způsobem. Obsah všech zpráv vytvořených v elektronické poště může být monitorován a prohlížen a v žádném případě jej nelze považovat za soukromé.

Při používání elektronické pošty je nutné mít na zřeteli, že není zcela zajištěna po technické ani právní stránce bezpečnost zpráv pohybujících se v síti Internet. Dále také to, že zpráva může být uložena na různých místech, postoupena dalším adresátům či zaslána ve slepé kopii. Z těchto důvodů nelze elektronickou poštou zasílat obzvláště důležité a důvěrné obchodní informace.

Zaměstnanci firemní elektronickou poštu používají i k soukromým účelům a zvyšují tak riziko k ohrožení jejich poštovní schránky a celého systému.

1.3.3 Přístup k Internetu

Síť Internet poskytuje nepřeberné množství informací, které mohou pomoci při obchodní a výrobní činnosti firmy. Pokud však nejsou informace získány ze spolehlivého zdroje na Internetu, musí být před použitím ověřeny jiným způsobem.

Přístup na Internet pomocí prostředků Federal-Mogul a. s. je poskytován pouze pracovníkům, kteří jej potřebují ke své práci a děje se na základě přidělených uživatelských jmen a hesel. Tato jména a hesla zabezpečuje oddělení informačních systémů na základě žádosti podepsané nadřízeným manažerem pracovníka.

Pověření uživatelé Internetu musí dodržovat pravidla předepsaná standardy Federal-Mogul Corporation, a to zejména:

- vyhnout se přístupu na stránky, které nemají souvislost s činností F-M,
- dbát na dodržování autorských práv, omezit přenos velkých souborů,
- chránit citlivé obchodní informace a nedůvěřovat bez ověření informacím získaných z Internetu,
- nesmí používat přístupu k Internetu k nelegálním účelům,
- používat cizí jména, hesla a klíče,
- používat programy omezující či obcházející instalovanou ochranu sítě,

- provozovat aktivity, které mohou poškodit síťové systémy, počítače či uložená data,
- stahovat nelicencovaný software,
- používat Internet ke hraní her či stahování her,
- prodávat nebo distribuovat software po Internetu,
- zveřejňovat osobní data zaměstnanců F-M,
- nesmí stahovat, ukládat, zasílat, záměrně přijímat či si vyměňovat pirátský software, ukradená hesla, ukradená čísla kreditních karet, neslušné či obscénní materiály nebo jakékoli jiné informace neslučitelné s obchodními cíli F-M.

Veškeré používání Internetu včetně elektronické pošty může být předmětem zkoumání a monitorování ze strany F-M, aby bylo možno ověřit správné použití těchto služeb, v souladu s politikou F-M, která stanoví, že žádná data uložená na firemních počítačích nejsou soukromá a nemohou být za soukromá považována.

1.3.4 Používaný software a licence

Federal-Mogul, a. s. připouští na svých počítačích používání výhradně licencovaného software. Všichni zaměstnanci musí být seznámeni s touto politikou a jsou zodpovědni za dodržování licenčních podmínek ke všem softwarům v souladu s autorským zákonem a ostatními souvisejícími zákony. Je výslovně zakázáno používání takového softwaru nad rámec licenčních podmínek, zejména jeho nelegální kopírování a rozmnožování.

Při pořizování nových počítačových systémů nebo aplikací zodpovídá vedoucí příslušného oddělení za zpracování návrhu technických požadavků. Tyto požadavky předloží IS organizaci k posouzení. IS organizace takový požadavek posoudí z hlediska vazeb na stávající a připravované systémy, z hlediska souladu se standardy F-M a z hlediska vhodnosti vybraného dodavatele. V případě neschválení návrhu musí zodpovědný vedoucí návrh přepracovat a znovu předložit ke schválení.

1.3.5 Antivirová ochrana

Antivirová ochrana musí být bezpodmínečně nainstalována na všech firemních serverech, počítačích i noteboocích, aby byla zajištěna ochrana těchto systémů před poškozením. Firemním standardem pro antivirovou ochranu je McAfee Anti-Virus. Datové soubory, obsahující informace o virech jsou pravidelně a automaticky aktualizovány.

1.3.6 Kontrola přístupu k systémům a aplikacím

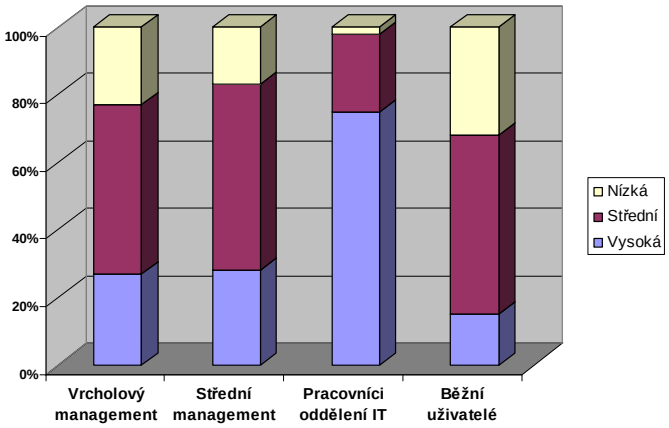
Určený správce každého systému definuje způsob přístupu jednotlivých uživatelů, založený na jedinečných uživatelských jménech a bezpečných heslech, aby bylo zamezeno ztrátě či zneužití těchto systémů a uložených dat. Na základě takto definovaných práv zajistí IS organizace přidělení jmen a příslušných práv. Správce každého systému je zodpovědný za průběžnou kontrolu dodržování. Přístupy jednotlivých uživatelů k systému jsou zaznamenávány.

1.3.7 Fyzické zabezpečení výpočetní techniky

Výpočetní technika a to zejména v místnosti, kde jsou umístěny servery a důležité části počítačové sítě, musí být náležitě zabezpečeny tak, aby se předešlo náhodnému či úmyslnému zničení či poškození. Zabezpečení místnosti serverů zahrnuje ochranu proti požáru, živelným pohromám či jiným přírodním vlivům, ochranu proti neoprávněnému vniknutí a kontrolu přístupu.

1.3.8 Úroveň povědomí o bezpečnosti informačních systémů

Následující graf znázorňuje jednotlivé úrovně povědomí o bezpečnosti dle úrovní řízení ve firmě. To dokazuje zjištění, že nejméně vzdělaní v bezpečnosti IS jsou běžní uživatelé systému firmy, jejichž povědomí je velice nízké.



Graf 2: Úroveň povědomí o bezpečnosti

1.4 Zálohování dat ve firmě

1.4.1 Proces zálohování

Zálohovací procedury vytváří IS organizace ve formě instrukcí, jejichž aktuální podoba je vždy k dispozici v centrální databázi ETS Site Documentation a musí být nastaveny tak, aby bylo zajištěno zálohování veškerých důležitých dat vytvořených uživateli v intervalech, které odpovídají rozsahu dat a jejich důležitosti.

Dále musí být minimálně jednou týdně zálohovány systémové informace na všech serverech. Zálohovací procedury pro jednotlivé systémy musí popisovat frekvenci, rozsah a způsob zálohování, včetně uvedení způsobu uložení zálohovacích médií.

Data ukládaná mimo podnik

Zálohy nejdůležitějších systémů, určené organizací IS musí být uloženy mimo podnik. Způsob uložení a přístup k zálohám zabezpečuje regionální koordinátor infrastruktury. Zálohy ostatních systémů musí být uloženy odděleně od serverů a zálohovaných stanic. Způsob zálohování a uložení záloh zabezpečuje správce

konkrétního systému či aplikace po odsouhlasení regionálním koordinátorem infrastruktury.

Druhy ukládaných dat

Mezi nejdůležitější systémy, které se zálohují a jsou uloženy mimo podnik patří elektronická pošta a ostatní databáze v Lotus Notes, z kterých se denně zálohuje cca 150 GB. Dále se zálohuje asi 50 GB na SQL serveru, jenž obsahuje data z personalistiky, hlavně mzdy. K denním zálohám patří i uživatelská data, soubory a sdílené adresáře apod. z Novell Evolution, které zaobírají zhruba 180 GB. ***Celkové množství ukládaných dat denně*** se tedy pohybuje okolo ***380 GB***.

Průběh zálohování

Zálohování je nastaveno v pracovní dny se začátkem kolem 22:00 hod. Firma zálohuje na pásky S-DLT 160/320. Zálohování celkově probíhá 4 – 5 hodin. Vše probíhá on-the-fly, tzn. že všechny systémy stále běží a ráno se pak zkontroluje, jak dopadla záloha z minulé noci. Pokud nastanou nějaké problémy, řeší se to jako top priority. Pokud je vše v pořádku, odvezou se pásky do Komerční banky v Kostelci nad Orlicí, kde se vyzvednou pásky z minulého dne a ty se uloží do trezoru firmy, který je mimo serverovou místnost. Z trezoru se vezmou pásky pro aktuální pracovní den a vloží se do serverů.

Pásky z konce měsíce se ukládají v podniku do trezoru, který je v jiné budově než server, a to na 12 měsíců, pásky z konce roku se ukládají do téhož trezoru a archivují se 5 let. Na konci pracovního týdne, tj. v pátek se ještě před zálohováním spouští čistící páska.

Zálohování informací uložených na všech serverech probíhá centralizovaně současně se zálohováním těchto systémů. Tyto zálohy zajišťuje koordinátor oddělení regionální infrastruktury.

Zálohování ostatních dat a aplikací je řešeno přímo na jednotlivých stanicích.

Zálohování aplikace a databáze MFG/PRO zajišťuje Datové centrum Federal-Mogul v Manchesteru, kde dochází k zálohování všech výrobních a účetních dat. Z hlediska firmy v Kostelci nad Orlicí není nutné tato data zálohovat.

Plán obnovy systému

V souvislosti s procedurami zálohování je zároveň nutné mít vypracovány plány obnovy systémů a dat z těchto záloh (Disaster Recovery Plan). Za vypracování plánů obnovy systému zodpovídá regionální koordinátor infrastruktury.

Disaster Recovery Plan musí být minimálně jednou ročně podroben kontrole a zaktualizován. Aktualizace musí také proběhnout zároveň s každou větší změnou systémů, kterých se dotýká. Aktuální verze plánů musí být uložena mimo podnik spolu se zálohami a dále její kopie musí být uložena u regionálního koordinátora infrastruktury a ředitele podniku.

Odpovědné osoby při zálohování dat

Správci jednotlivých systémů zodpovídají za přípravu, nastavení a dodržování zálohovacích procedur na jednotlivých systémech a za uložení zálohovacích médií mimo zálohovaný systém.

Regionální koordinátor infrastruktury zodpovídá za zajištění zálohování systémových informací na serverech minimálně jednou týdně a za vypracování plánu obnovy systémů a dat na serverech.

1.4.2 Zálohovací zařízení

Zálohovací mechaniku SDLT 320 Federal-Mogul, a. s. používá od firmy Hewlett Packard. SDLT 320 patří do druhé generace mechanik Super DLT a umožňuje uložit až 160 GB dat bez komprese a 320 GB s kompresí při dosažení rychlosti 16 resp. 32 MB/s. Zálohování dat bez komprese probíhá rychlostí 57,6 GB/hod se zpětným čtením kompatibility předchozích generací SDLT a DLT médií. Toto zařízení nepracuje

jako tzv. autoloader, pásky se musí vkládat ručně. Jedná se o starší typ, který již v současné době nelze zakoupit.

1.5 Obnova IS

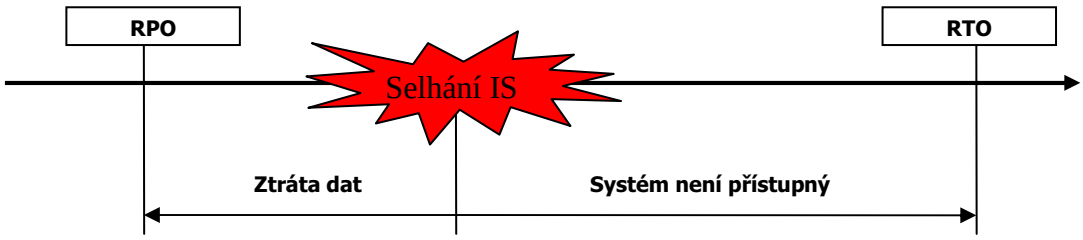
Vlastní obnova informačního systému není předmětem této práce. Zaměřuji se pouze na obnovu dat.

V současné době firma používá zálohovací pásky pro obnovení dat, která si jednotliví uživatele odstraní z počítače svým nedbalým přičiněním. K totální obnově dat dochází v poslední době zhruba jednou za dva roky. Naposledy se tomu ve firmě stalo v roce 2005.

1.5.1 Business Continuity Plan

Business Continuity Plan se zabývá problémem, jak pokračovat v chodu firmy v případě selhání počítačového systému. Tento plán je ve firmě omezen na počítače, tiskárny, síť a připojení k síti MAN.

Cílem každého oddělení ve firmě je mít připravený tzv. "papírový" systém, který musí být schopný řešit dva hlavní úkoly, mezi které patří pokrytí období, kdy se systém snaží obnovit a znovu získání ztracených dat mezi poruchou a posledním zálohováním. Zastavení činností ve firmě není žádnou volbou.



Obrázek 4: Průběh selhání IS[3]

[3] *Disaster Recovery Plan Risk & Impact Analysis*. Kostelec nad Orlicí. 2005. s. 1

1.5.2 Disaster Recovery Plan

Disaster Recovery Plan (havarijní plán a plán obnovy IS) ve firmě existuje a je pravidelně testovaný. Jeho platnost je vždy v dubnu. Jeho cílem ve firmě je zdokumentování procedur a přiřazení povinností na obnovení systémů, které jsou efektivní součástí hlavních obchodních funkcí.

Povolená doba pro *RTO (Recovery Time Objective)*, znamená čas od výpadku po obnovení systému a ve firmě činí dva dny.

RPO (Recovery Point Objective), zachycuje časový okamžik, ve kterém je dostupný poslední konzistentní stav dat. Nepřímo určuje maximální objem dat, která jsou ztracena v případě výpadku. Povolená doba RPO ve firmě je od posledního zálohování dat max. do jednoho dne. Během období obnovení dat, nemůže být očekávána žádná IT podpora.

Oblasti působnosti Disaster Recovery Plan ve firmě

Disaster Recovery Plan zahrunuje:

- obchodní rozhodující úlohy provedené použitím MFG/PRO nebo jinými počítačovými systémy (tisk faktur, dodacích listů, dodavatelů atd.),
- záznamy pohybu zásob, vedení účetnictví, výplatní listiny zaměstnanců,
- data, které podléhají archivaci,
- jakost a požadavky zákazníků,
- důležitá osobní telefonní čísla zaměstnanců,
- postup pro pozdější ukládání dat (pořadová čísla).

1.6 Závěr analýzy firmy

V praktickém pohledu správy uživatelů firmy se objevuje fakt, že se zaměstnanci z důvodu přihlašování do více systémů snaží svoji práci zjednodušit tím, že používají hesla, která si jsou např. příliš podobná, obsahují jména rodinných příslušníků, zaměstnanci je tvoří stále na stejném principu atd. V tom ale samotní pracovníci nevidí žádný problém.

V případě zacházení s elektronickou poštou zaměstnanci nepostupují správně. Zaměstnanci netuší, jakým rizikem pro ně a hlavně celý informační systém může být otevření e-mailu od neznámé osoby, která se do systému snaží nabourat nebo do něho zanést jakýkoliv malware[4], aby se nevědomky šířil dál.

I přesto, že se firma snaží samotné systémy stále zdokonalovat, největší roli na těchto systémech představují jejich uživatelé – zaměstnanci. Všechny tyto problémy pramení v neznalosti a celkově špatném povědomí o firemní bezpečnosti celých informačních systémů. Pracovníci jsou nedostatečně školeni. Veškeré školení probíhá na základě pouhého přečtení si prezentace o bezpečnosti na firemní síti, kde se pro zaměstnance nevyskytuje dostatek informací a nikdo s nimi problém bezpečnosti nekonzultuje a neprohlubuje jejich znalosti.

Dalším problém firmy je současné zálohování dat ve firmě, které neodpovídá potřebám a to proto, že množství zálohovaných dat má stále rostoucí tendenci a stávající mechanika určená pro pásky, které pojmou s kompresí 320 GB dat není dostačující. Potřeby firmy jsou v současné době 380 GB dat. Technologie zálohování nabízí nové možnosti, kterých by firma měla využít a snížit tak riziko, ke kterému může dojít při havárii informačního systému.

Největším nebezpečím je tedy pro firmu ztráta dat z pohledu nevyhovujícího zálohovacího hardwaru, který není schopen plnit požadavky firmy a nedostatečně proškolení zaměstnanci.

[4] **Malware** je počítačový program určený ke vniknutí nebo poškození počítačového systému. Pod souhrnné označení malware se zahrnují počítačové viry, trojské koně, spyware a adware.

2 Teoretická východiska práce

2.1 Bezpečnost v informačních systémech

Systém je tak bezpečný, jak je bezpečný jeho nejslabší článek.

Data patří k tomu nejcennějšímu, co organizace vlastní. Z dat se interpretací do souvislostí firemního obchodu stávají informace, které jsou každý den vystaveny mnoha rizikům jako je zničení, ztráta, poškození, zcizení atd.

Některá tato data lze označit jako citlivé, např. osobní záznamy zaměstnanců, interní údaje o klientech, finanční údaje firmy, zdravotní záznamy pacientů a mnoho dalších. Tyto zdroje je proto nesmírně důležité odpovídajícím způsobem zabezpečit a chránit.

Budování bezpečnosti informačních a komunikačních technologií (ICT) je během na "dlouhou trať". Tento firemní proces je třeba chápat v širších souvislostech - nejen technických, ale také organizačních, personálních, právních, sociálních a dalších. O technických komponentách bezpečnosti je třeba uvažovat v souvislosti s ostatními aspekty bezpečnosti ICT. Jen tak se může podařit zajistit nezbytnou důvěryhodnost informačních technologií (IT) struktur organizace.

Čím dál větší rozmach informačních systémů (IS), jenž zasahuje do všech oblastí lidského života, zvyšuje riziko napadení těchto systémů, a to ať je to napadení záměrné, náhodné nebo nějaká chyba, případně neznalost.

2.1.1 Komponenty IS

Chápejme IS jako soubor následujících komponent:

1. Technické prostředky (hardware) – počítačové systémy doplněné o periferní jednotky, např. servery, procesory, paměti, atd.
2. Programové prostředky (software) – jsou tvořené systémovými programy, které řídí chod počítače, efektivní práci s daty, komunikaci počítačového systému s reálným světem a programy aplikačními.

3. Datové zdroje – ke své práci je využívají programové prostředky.
4. Organizační prostředky (orgware) – soubor nařízení a pravidel. Ty definují provozování a využívání IS/IT.
5. Lidé (peopleware) – řeší otázky adaptace a účinného fungování člověka v počítačovém prostředí, do kterého je zasazen, např. správci systémů, uživatelé, obsluha a další osoby, které bezprostředně přicházejí do styku s IS.
6. Reálný svět (informační zdroje, legislativa, normy) – kontext IS.

Tyto prvky můžeme označit jako ***aktiva***, protože pro firmu provozující IS představují konkrétní hodnotu. Současně by měla být určena zodpovědnost za jejich ohodnocení. Proto je nutné určit a přijmout určité role správců, uživatelů apod., čímž se zabývá bezpečnostní politika.

Analyzujeme-li IS z hlediska zabezpečení, rozpoznáváme tyto komponenty dle jejich aktivit v IS:

- *„objekt IS - pasivní entita, která obsahuje/přijímá informace a je přístupná autorizovaným[5] subjektům IS*
- *subjekt IS - aktivní entita (osoba, proces nebo zařízení činné na základě příkazu uživatele) autorizovatelná pro získání informace z objektu, vydávání příkazů ovlivňujících udělení práv přístupu k objektu, změnu stavu objektu apod.*

Důvěryhodný IS (subjekt nebo objekt) je taková entita, o které se věří (je o tom podán důkaz), že je implementovaná tak, že splňuje svoji specifikaci vypracovanou v souladu s bezpečnostní politikou. Na důvěryhodnou entitu se můžeme spolehnout, chová-li se tak, jak očekáváme, že se bude chovat.“[6]

[5] ***Autorizace*** subjektu pro jistou činnost rozumíme určení, že daný subjekt je z hlediska této činnosti důvěryhodný. Udělení autorizace subjektu si vynucuje, aby se pracovalo s autentickými subjekty. ***Autentizací*** se rozumí proces ověřování pravosti identity entity (subjektu, objektu, tj. uživatele, procesu, systémů, informačních struktur apod.).

[6] HANÁČEK, P. a STAUDEK, J. *Bezpečnost informačních systémů*. 1. vyd. Praha: Úřad pro státní informační systém. 2000. s. 12-13. ISBN 80-238-5400-3

2.1.2 Bezpečnostní politika

Bezpečnostní politika, hlavně firemní, by měla být chápána jako určitý souhrn principů a jejich východisek pro strategické řešení situací. Každá firma působící v IT by si měla stanovit celkovou bezpečnostní politiku, ze které poté bude vycházet bezpečnostní politika pro IS. Ve fázi celkové bezpečnostní politiky se stanoví mj. bezpečnostní cíle na úrovni vrcholového managementu, jenž se určí na základě rizikové analýzy.

Bezpečnostní politika představuje výchozí body pro návrh a realizaci všech firemních standardů, směrnic, procedur a opatření, které jsou ve firmě nezbytné.

Dokument politiky je všeobecný plánem, na jehož základě se všechny informace získávají a využívají. Definuje oblasti, ve kterých je nutné tento proces řídit a kontrolovat.

Politika by měla odpovědět při nejmenším na tyto otázky:

- *Co musí být chráněno?*
- *Kdo za to nese zodpovědnost?*
- *Kdy to bude efektivní?*
- *Jak to bude vynuceno?*
- *Kdy a jak to bude uvedeno do praxe?*

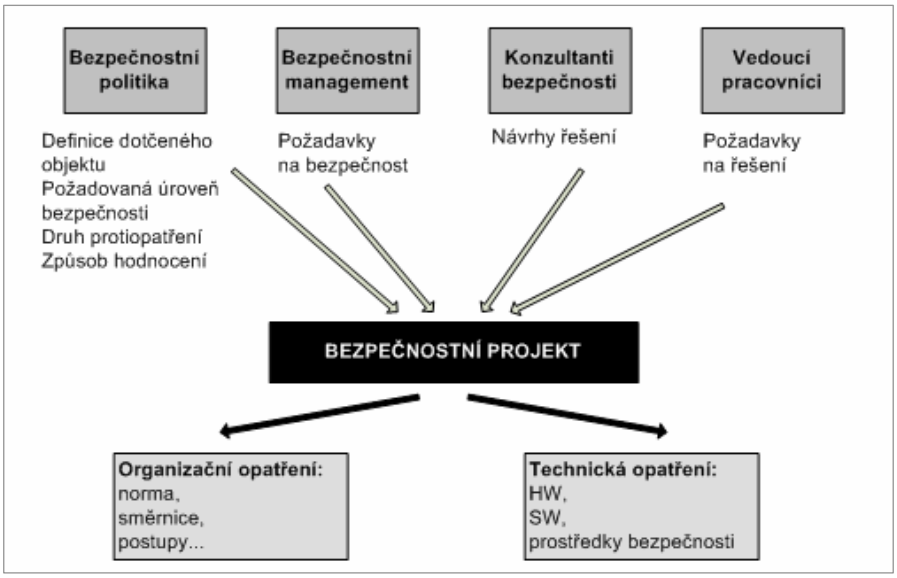
Je velice důležité si uvědomit, že poté může ve firmě docházet ke střetu dvou aktivit, mezi které patří bezpečnostní a obchodní cíle. Tyto cíle nejsou spolu totožné a obecně se vzájemně ani nepodporují. Přesto cíle bezpečnostní musí být vstřícné obchodním cílům.

2.1.3 Bezpečnostní projekt

Bezpečnostní projekt představuje konkrétní požadavky na provedení určitých činností. Nejlépe představitelným bezpečnostním projektem pro fyzickou ochranu je např. fakt, že k hlavním dveřím objektu postavíme strážného a na zadní dveře dáme petlici a zámek.

Informační bezpečnost se musí dodržovat systematicky, tzn. neustále. Nestačí občasné školení zaměstnanců o tom, co to bezpečnost je nebo školení uskutečněné až po vzniku bezpečnostního incidentu. Cesta ke komplexní bezpečnosti je vyhodnocení účinnosti a trvalého školení.

Každý bezpečnostní projekt lze definovat jako určité vstupy a výstupy.



Obrázek 5: Bezpečnostní projekty[7]

2.1.4 Zranitelné místo, hrozba a riziko

Zranitelným místem rozumíme slabinu IS, jenž lze využít ke způsobení škod nebo ztrát, dojde-li k útoku na IS. Tyto slabiny vznikají důsledkem chyb, selhání analýzy, v návrhu a/nebo implementaci IS. Správnou analýzou zranitelných míst,

[7] RODRYČOVÁ, D. a STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy*. 1. vyd. Praha: Grada. 2002. s. 35 ISBN: 80-7169-144-5

vytvořením bezpečnostní politiky a implementací všech bezpečnostních funkcí snižujeme pravděpodobnost úspěšného útoku na IS.

Zranitelná místa se vyskytují :

- ve fyzickém uspořádání,
- v organizačních schématech,
- v administrativních opatřeních,
- v personální politice, správě nebo managementu organizace,
- v logických a technických opatřeních ad.

Pojmem *hrozba* označujeme potenciální možnost zneužití zranitelného místa v IS k útoku na tento IS. Útok probíhá za účelem způsobení škody na aktivech nebo jejich úplném zničení.

Hrozby lze dělit na:

1. objektivní – bez lidského přičinění
    - přírodní, fyzické (požár, výpadek napětí, …)
    - fyzikální (elektromagnetické vyzařování, ...)
    - technické nebo logické (nefunkčnost paměťového média, porucha paměti, …)
2. subjektivní - plynoucí z lidského faktoru
    - neúmyslné (neznalost uživatele, …)
    - úmyslné (útočník, konkurence, …)

Riziko představuje vztah pravděpodobnosti využití zranitelného místa útočníkem nebo uživatelem IS a dopadu uskutečnění této hrozby. Riziko lze popsat následujícím vztahem:

***RIZIKO** = dopad využití zranitelnosti * pravděpodobnost hrozby*

2.1.5 Bezpečnostní funkce a mechanismy

Při pohledu na IS a jeho zabezpečení je nutné prvně stanovit *bezpečnostní cíle* a způsob jejich dosažení. Bezpečnostní cíle jsou jedny z dílčích přínosů bezpečnosti, kterou dosahuje IS z hlediska udržení důvěrnosti, integrity a dostupnosti. Abychom cílů dosáhli, aplikuje se jejich používání na funkce prosazující bezpečnost, tzv. *bezpečnostní funkce.*

Bezpečnostní mechanismy implementují bezpečnostní funkce. Jedná se o mechanismy navržené tak, aby detekovaly útoky, zabraňovaly jim, eventuelně pomohly zotavení se z útoků.

Dle jejich **rozsahu** člením bezpečnostní mechanismy na:

- slabé bezpečnostní mechanismy - ochrana před amatéry, proti náhodným útokům, lze je narušit kvalifikovaným útokem, tj. útokem střední síly
- bezpečnostní mechanismy střední síly - ochrana před hackery, proti úmyslným útokům s omezenými příležitostmi a možnostmi, hovoříme o běžných útocích
- silné bezpečnostní mechanismy - ochrana před profesionály, ochrana proti útočníkům s vysokou úrovní znalostí, s velkými příležitostmi a prostředky, použité útoky se vymykají běžné praxi.

Ne méně podstatná je kategorizace těchto mechanismů podle **technologického hlediska**, kterou lze přiblížit takto:

- softwarové (logické) bezpečnostní mechanismy

  Jedná se o mechanismy, které určují princip řízení přístupu v daném operačním systému. Jednou z oblastí, jenž se touto problematikou zabývá je *kryptografie* a to jak symetrická, v které se pracuje s tajným klíčem nebo asymetrická, kdy se použije veřejný a privátní klíč. Mezi další mechanismy patří standardy pro návrh, kódování, testování, údržba programů, ochranné nástroje v operačních systémech, např. ochrana paměti, ochrana souborů řízením přístupu, obecná ochrana objektů, tj. přístupové matice, přístupové seznamy,

hesla, autentizace přístupu k terminálu, mechanismy určené pro autentizaci zpráv.

- hardwarové (technické) bezpečnostní mechanismy

  Do této skupiny lze zařadit např. šifrovače a autentizační a identifikační karty.

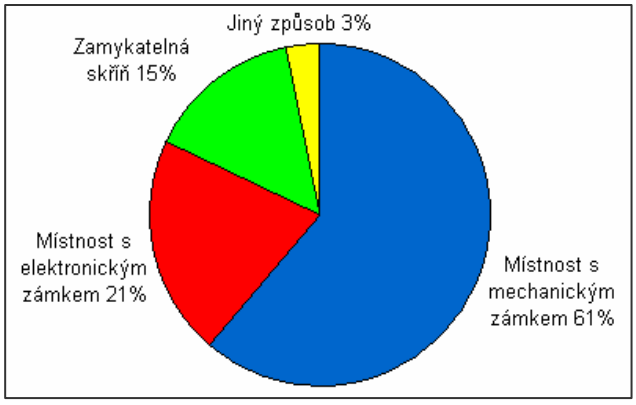
- fyzické bezpečnostní mechanismy

  Např. trezory, zámky, stínění, protipožární ochrana, generátory náhradní energie, chráněná místa pro záložní kopie dat a programů.

- administrativní bezpečnostní mechanismy

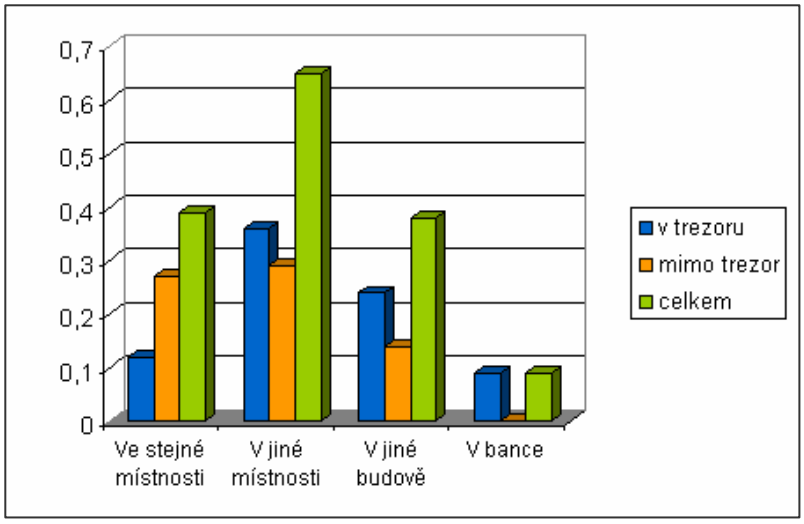
  Zde je velice důležitý výběr důvěryhodných osob, správně zvolená silná hesla, právní normy, zákony, vyhlášky, předpisy ad.

Následující grafické ukázky znázorňují fyzické bezpečnostní mechanismy ve firmách a jakým způsobem firmy ukládají záložní nosiče informací. Největší podíl uložení nosičů zaujímá uložení v trezoru firmy, který se nachází v jiné místnosti. Na nejhorší pozici se nachází média uložená v bance.



Graf 3: Fyzické zabezpečení[8]

[8] RODRYČOVÁ, D. a STAŠA, P.. *Bezpečnost informací jako podmínka prosperity firmy*. 1. vyd. Praha: Grada. 2002. s. 22. ISBN: 80-7169-144-5



Graf 4: Uložení záložních nosičů informací[9]

2.2 Bezpečnostní normy

V posledních letech význam mezinárodních norem (standardů) neustále roste a firmy jimi prokazují svoji způsobilost k provádění své činnosti, tudíž se také zajímají o certifikace norem neboli prokázání souladu.

2.2.1 Mezinárodně uznávané normy

„Podle českého právního řádu jsou všechny normy pouze doporučené, není-li (ve výjimečných případech) zákonem stanoveno jinak. Existuje celá řada národních i mezinárodních organizací, které se vydáváním norem zabývají profesionálně a platí ve svém oboru za uznávanou autoritu. Řada norem těchto organizací je přebírána českým úřadem, samozřejmě po důsledném překladu do českého jazyka.“[10]

[9] RODRYČOVÁ, D. a STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy*. 1. vyd. Praha: Grada. 2002. s. 22. ISBN: 80-7169-144-5

[10] DOSEDĚL, T. *Počítačová ochrana a ochrana da*t. 1. vyd. Brno: Computer Press. 2004. s. 141 – 142. ISBN: 80-251-0106-1

Nejčastěji se můžeme setkat s těmito normami:

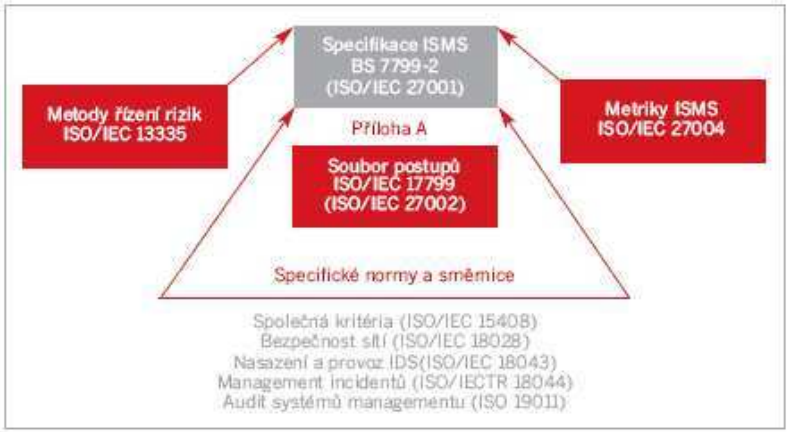
- **normy ISO:** vydává International Organisation for Standardisation,
- **normy IEC:** vydává International Electrotechnical Commision,
- **normy ITU:** vydává International Telecommunication Union.

2.2.2 Normy managementu bezpečnosti informací ISO

V této práci jsem se soustředila na bezpečnost podle nejnovější normy ISO 17799:2005, dále existují další normy, kterými se bezpečnost IS řídí, a to ISO/IEC 15408 (Common Criteria), ISO/IEC TR 13335, apod.

Na jaře roku 2005 organizace ISO ohlásila zavedení nové série norem ISO 27000, která se bude věnovat problematice managementu bezpečnosti informací. Právě tato skutečnost prohlubuje již existující snahy o jasné vymezení vztahů a hranic mezi bezpečnostními normami.

10. června 2005 uveřejnila mezinárodní organizace pro normalizaci ISO aktualizovanou verzi normy ISO/IEC 17799:2005 – Code of practice for information security management (Soubor postupů pro management bezpečnosti informací). Není to jediná změna ISO v oblasti bezpečnosti v roce 2005. Vznikla také norma ISO/IEC 27001:2005 – Information security management system – Requirements (Systém managementu bezpečnosti informací – Požadavky). Tyto normy ISO jsou oficiální podobou britského standardu BS 7799-2.



Obrázek 6: Koncept série ISO 27000 [11]

[11] /online/ NOVÁK, L. a ZAPLETALOVÁ, V. *Nová série bezpečnostních norem.* DSM. 2005. Dostupné z: http://www.dsm.tate.cz, převzato 3. 5. 2007

2.2.3 Oblasti normy ISO 17799:2005

Norma ISO 17799:2005 má v oblasti počítačové bezpečnosti mimořádně široký, vyčerpávající záběr a obsahuje množství kontrol uspořádaných do deseti různých oblastí:

1. ***Řízení kontinuity činnosti organizace..*** Popisuje možnosti pokračování činnosti podniku i po zásadním selhání či havárii.

2. ***Řízení přístupu.*** Vymezuje řízení a přístup k informacím veškerého druhu v dané organizaci a zejména detekci neoprávněných aktivit.

3. ***Akvizice, vývoj a údržba informačních systémů.*** Hovoří o procesu ochrany aktiv a o začlenění principů bezpečnosti do všech stránek informačních systémů, softwaru a dat organizace.

4. ***Fyzická bezpečnost a bezpečnost prostředí.*** Brání v neoprávněném přístupu či poškození systémů, bez ohledu na záměry rušitele.

5. ***Soulad s požadavky.*** Organizace si prostřednictvím auditu ověří, jestli nenarušuje žádné zákonné a podzákonné normy, předpisy či smluvní závazky, a zjistí případné bezpečnostní požadavky.

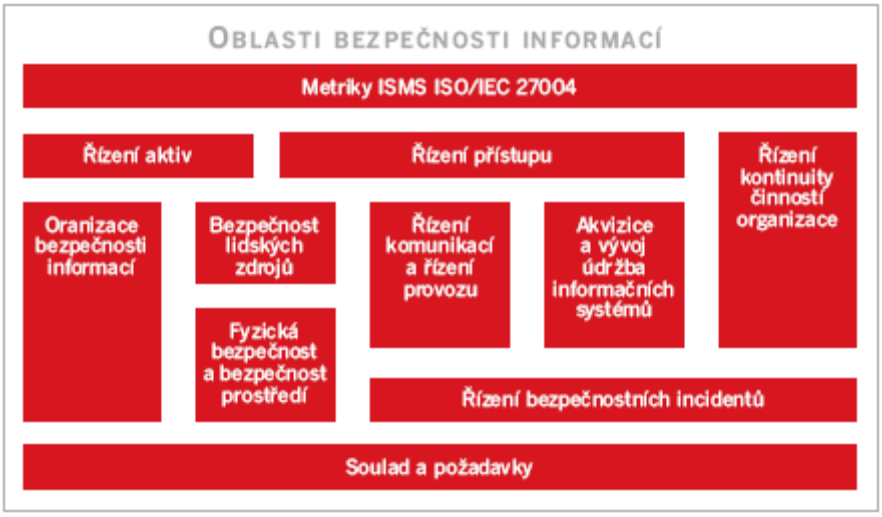
6. ***Bezpečnost lidských zdrojů.*** Rozebírá možnosti snížení rizika lidské chyby, krádeže nebo zneužití systémů, a tím pádem i rizika poškození a nesprávné funkce při bezpečnostních incidentech; hovoří také o výsledném ponaučení z incidentů.

7. ***Organizace bezpečnosti informací.*** Vymezuje způsoby řízení a udržování bezpečnosti informací v dané firmě či organizaci.

8. ***Řízení komunikací a řízení provozu.*** Uvádí metody, které vedou k minimalizaci rizik za současného zvýšení bezpečnosti a prováděné s ohledem na střežení informací a ochranu před ztrátou, neoprávněnou modifikací či zneužitím.

9. ***Řízení aktiv.*** Popisuje udržování potřebné ochrany podnikových aktiv a zajišťuje odpovídající úroveň ochrany i pro informační aktiva.

10. ***Řízení bezpečnostních incidentů.*** Cílem této části je poskytnout směr a podporu na bezpečnost informací.



Obrázek 7: Nové rozdělení oblastí bezpečnosti informací[12]

[12] /online/ NOVÁK, L. a ZAPLETALOVÁ, V. *Nová série bezpečnostních norem.* DSM. 2005. Dostupné z: http://www.dsm.tate.cz, převzato 3. 5. 2007

2.2.4 Přehled změn ISO 17799:2005

Oblast bezpečnosti	Cíle			Opatření / kontroly		
	2005	2000	Změna	2005	2000	Změna
Bezpečnostní politika	1	1	0	2	2	
Organizace bezpečnosti informací	2	3	-1	11	10	+1
Řízení aktiv	2	2	0	5	3	+2
Bezpečnost lidských zdrojů	3	3	0	9	10	-1
Fyzická bezpečnost a bezpečnost prostředí	2	3	-1	13	13	0
Řízení komunikací a řízení provozu	10	7	+3	32	24	+8
Řízení přístupu	7	8	-1	25	31	-6
Akvizice, vývoj a údržba informačních systémů	6	5	+1	16	18	+2
Řízení bezpečnostních incidentů	2	0	+2	5	0	+5
Řízení kontinuity činností organizace	1	1	0	5	5	0
Soulad s požadavky	3	3	0	10	11	-1
Celkem	39	36	+3	133	127	+6

Tabulka 2: Přehled změn ISO/IEC 17799:2005 podle jednotl. oblastí bezpečnosti[13]

2.3 Obnova informačního systému

„Následky ztráty dat bývají pro firmy katastrofické.
94% firem, které postihne těžká ztráta dat ukončí do 3 měsíců svou činnost,
neboť nejsou schopny na trhu přežít.“[14]

Samotná bezpečnost IS závisí přímo s jeho obnovou. Kdyby systému nehrozily takové hrozby, se kterými se stále potýká, obnova systému a dat by nebyla za potřebí. Proto je nutné mít vypracované plány, které se obnovou systému zabývají a data zálohovat, abychom je měli z čeho obnovit.

[13] /online/ NOVÁK, L. a ZAPLETALOVÁ, V. *Nová série bezpečnostních norem.* DSM. 2005. Dostupné z: http://www.dsm.tate.cz, převzato 3. 5. 2007

[14] *Zdroj: PC Today*

2.3.1 Plánování kontinuity činností

Plánování kontinuity činností lze definovat jako souhrn aktivit zaměřených na snížení rizika vzniku havárie a omezení dopadů havárie na kritické podnikové procesy. Důležité je si uvědomit, že plánování kontinuity není jen plánem reakce na krizovou událost, ale obsahuje také důležitý preventivní aspekt. Jedním z hlavních výstupů tohoto procesu je plán zachování kontinuity činností, tzv. Business Continuity Plan. Kvalitní plány kontinuity činností jsou schopny minimalizovat následky mimořádných událostí a zároveň umožňují a urychlují uvedení provozu do normálního stavu.

Životní cyklus BCP má následující strukturu:

1. Analýza
2. Návrh strategie kontinuity
3. Implementace plánů kontinuity
4. Testování a údržba
5. Reakce na havárii
6. Produkty podporující BCP

Kvalitní zpracovaní plánů kontinuity činností by mělo být strategickým cílem jakékoliv organizace - od velkých nadnárodních společností až po malý či střední podnikatelský subjekt. I když se masivnost nasazení konkrétních technologií bude v organizacích různého typu lišit, je nutné zachovat při navrhování plánů kontinuity stěžejní principy životního cyklu řízení kontinuity.

2.3.2 Disaster Recovery Plan - Havarijní plán a plán obnovy IS

Havarijní plán a plán obnovy IS (plán pro zvládání krizových situací a plán obnovy) stanovuje postupy, které budou uplatněny v případě mimořádné události, jako jsou havárie, živelné pohromy, katastrofy a bezpečnostní incidenty, jež ohrožují provozuschopnost IS. Tyto plány se zabývají požadavky na zachování kontinuity

provozu, stanovují kritické lhůty pro obnovu, definují příslušné náhradní řešení, specifikují postupy při zálohování, upřesňují jednotlivé role zaměstnanců při haváriích, jejich pravomoci, odpovědnosti a postupy při obnově dat.

2.3.3 Zálohování

Nejspolehlivějším způsobem, jak obnovit systém po jakékoli události, je ze záloh. Zálohování je proces kopírování dat na jiné místo nebo jiný druh nosiče. Původní data zůstávají. Data bývají ze záložní kopie později obnovena, jestliže počítačový systém postihne nějaká pohroma nebo útok. Proces zálohování lze nastavit na část disku nebo celý disk.

Základem systematického zálohování podnikových dat je stanovení rotačního schématu záložních médií. Je důležité, aby bylo zaručeno uchování dat po dobu více než jednoho dne. Cílem je zajistit co nejdelší a maximálně různorodé kopie dat. Současně je nutno zálohy zabezpečit – fyzicky i symetrickým šifrováním, které standardně zálohovací programy umožňují.

Metody zálohování

Plná záloha (full backup) zkopíruje všechny vybrané soubory na záložní médium a označí je jako zálohované. Toto označení provádí zálohovací program, který všem souborům vynuluje nastavení archivního atributu. Archivní atribut zůstává automaticky přidělen operačním systémem souborům, jenž byly nově vytvořeny nebo došlo k jejich přejmenování, eventuálně k otevření pro zápis. Jednoduše řečeno, během změny stavu souboru se vygeneruje tento atribut. Tento druh zálohy je nejjednodušší variantou a rovněž obnova dat je velmi snadná.

U zálohy typu ***přírůstková (incremental)*** jsou zálohována pouze data, u nichž je nastaven atribut archive, přičemž tento atribut je u nich po zálohování odstraněn. Zálohují se tak pouze data, která byla změněna či u kterých byl od poslední plné zálohy ručně nastaven atribut archive. Záloha je podstatně kratší než u plné zálohy, proto se používá zpravidla pro zálohování během pracovního týdne. V případě havárie serveru nebo diskového pole je nutné nejprve obnovit poslední plnou zálohu a posléze

v časovém sledu všechny zálohy přírůstkového typu. Z toho vyplývá, že inkrementální zálohy jsou sice rychlejší na vytvoření, čas obnovy je však díky nutnosti obnovy z několika různých zálohovacích sad delší.

Rozdílová záloha (differential) pracuje tak, že jsou zálohována pouze data, u nichž je nastaven atribut archive**,** přičemž tento atribut u nich není po zazálohování odstraněn. Zálohují se tak pouze ta data, která byla změněna či u nich byl od poslední plné zálohy ručně nastaven atribut archive**.** Záloha je podstatně kratší než u normální zálohy**,** proto ji lze podobně jako u inkrementální zálohy používat pro zálohování během pracovního týdne. Ze zálohy tytu differential také nepostačuje pro obnovu do původního stavu obnova pouze této zálohy. V případě havárie serveru či diskového pole je nutné nejprve obnovit poslední zálohu typu full backup a posléze v časovém sledu poslední zálohu rozdílového typu v období po poslední plné záloze. Z toho vyplývá, že rozdílové zálohy jsou z pohledu vytvoření srovnatelně rychlé jako inkrementální, čas obnovy je díky nutnosti obnovit pouze jedinou diferenciální zálohu kratší, přičemž zde je patrná závislost na tom, kolik nekompletních záloh od poslední plné zálohy proběhlo.

Velmi blízko k normální metodě má samotné ***kopírování (copy)***. Intuitivně se jedná o zkopírování všech vybraných souborů, ovšem hodnota archivního atributu se nemění. Tuto metodu lze použít mezi normální a inkrementální zálohou, protože nijak neovlivňuje a nezasahuje do běžícího zálohovacího procesu.

Pro zálohování dat vytvořených nebo změněných během dne slouží denní záloha, takže dochází k zálohování informací s datem úpravy shodným se zálohovacím dnem. Dostane-li zálohovací program za úkol zálohovat pouze změněné soubory, jednoduše se orientuje podle již zmiňovaného archivního atributu, hledá data s nastaveným atributem.

	Zálohuje	Maže A
Normal	Vše	ANO
Incremental	Jen A	ANO
Differential	Jen A	NE
Copy	Vše	NE
Daily	Jen A (včera)	ANO

Tabulka 3: Metody zálohování[15]

[15] Značkou ***A*** se rozumí archivní atribut.

Způsoby zálohování

On-line záloha (průběžná) – zálohování probíhá neustále a nepřetržitě za plného provozu systému do jiného datového úložiště s cílem zajištění dostupnosti dat. Během zálohování všechny databáze stále běží. Vytváření kopie dat a zápis dat na zálohovací zařízení je časově náročná úloha. Doba, po kterou je aplikace nečinná z důvodu zálohování se nazývá zálohovací okno (backup window). S nárůstem dat narůstá i těchto zálohovacích oken. On-line zálohování představuje výrazně nižší riziko ztráty dat než off-line zálohování.

Off-line záloha (záloha v době mimo provoz) – tento způsob zálohování vyžaduje zastavení činnosti systému, tudíž dochází k vytváření kopií určitého stavu dat a jeho ukládání opět na jiné diskové úložiště. Na rozdíl od on-line zálohování bude ztráta znamenat výpadek, nutnost nahrání zálohovaných dat a znovu zprovoznění serveru. Data nemusí být v tom stavu, v jakém byla při výpadku.

3 Vlastní návrh řešení

Tato část vychází z části analytické. Jak vyplynulo z analytických a teoretických poznatků, největším nebezpečím jsou pro firmu z pohledu bezpečnosti firmy nezodpovědní zaměstnanci a hardware zálohování. Proto se následující dvě podkapitoly budou věnovat těmto problémům.

První kapitola *Budování povědomí zaměstnanců o bezpečnosti firmy* se skládá z všeobecných požadavků na zaměstnance, navrhované klasifikace informací a dokumentů firmy, fyzické bezpečnosti a bezpečnosti prostředí, zacházení s hardwarovým a softwarovým vybavením z pohledu zabezpečení, kontroly přístupu k systému, používání firemního e-mailu a navrhovaného školení zaměstnanců. Jedná se o bezpečnostní opatření, která by měla být ve firmě z důvodu bezpečnosti dodržována. Jak vyplývá z analýzy firmy, některá všeobecná pravidla bezpečnosti ve firmě platí, ta která budou zmíněna v této části budou konkrétnější a propracovanější.

Druhá kapitola se zabývá návrhem nového zálohování ve firmě, v kterém navrhnu požadavky na zálohování a na jejich základě vyberu způsob a metodu zálohování dat a zálohovací zařízení.

3.1 Budování povědomí zaměstnanců o bezpečnosti firmy

Ve firmě by mělo dojít k podstatnému zlepšení znalostí bezpečnosti, se kterou se zaměstnanci denně setkávají. Můj návrh zahrnuje nejdůležitější problémy zabezpečení ve firmě. Cílem je vysvětlení zaměstnancům, jak by se měli z pohledu bezpečnosti chovat na firemní informační síti i mimo ni, jaké jsou jejich odpovědnosti a pravomoci, co je bezpečnostní politikou firmy. Toto vzdělávání by mělo probíhat na bázi školení zaměstnanců pracujících s počítačem, školení by se mělo pravidelně opakovat a případně prohlubovat.

S následujícími navrhovanými zásadami bezpečnosti doporučuji seznámit zaměstnance již při podpisu pracovní smlouvy, kdy musí zaměstnanec podepsat *Směrnici bezpečnosti informačních systémů* a projít školením o této bezpečnosti ještě

dříve, než mu budou udělena přístupová práva do systému firmy. Svým podpisem zaměstnanec stvrzuje souhlas a dodržování pravidel stanovených touto směrnicí.

Působnost všech následujících zásad navrhuji pro všechny zaměstnance, kteří přijdou do styku s IS firmy. Za odpovědnou osobu za vypracování následující směrnice navrhuji regionálního koordinátora infrastruktury IS[16].

Navrhuji, aby nedodržování *Směrnice bezpečnosti informačních systémů* i dalších jiných strategií firmy vedlo k pozastavení přístupu k systému firmy, disciplinárnímu řízení nebo při opakovaném porušení směrnice dokonce k rozvázání pracovního poměru.

3.1.1 Návrh zásad ochrany informací společnosti

Ohledně všeobecných zásad ochrany informací firmy navrhuji tato konkrétní řešení:

- každý zaměstnanec musí brát na vědomí a souhlasit se svou povinností ochrany informací,
- být zodpovědný za přiměřené a řádné používání informačních systémů,
- dodržovat zásady zabezpečení firemních informací,
- dodržovat procedury a směrnice firmy a další specifické instrukce pro zajištění bezpečnosti, které jsou dány vedením společnosti,
- všichni zaměstnanci, kteří přijdou do styku s informačním systémem musí absolvovat v rámci vstupního školení kompletní školení o bezpečnosti IS, kde se seznámí se strategiemi zabezpečení informací ve firmě,
- každý zaměstnanec může mít přístup pouze k těm informacím, které potřebuje pro svou práci.

[16] Regionálním koordinátorem infrastruktury IS se v této firmě rozumí funkce vedoucího IS, která je zde již takto zavedena.

Navrhuji takovouto odpovědnost, kontrolu a dokument k dodržování předešlých zásad:

Osoba odpovědná za dodržování [17]:	zaměstnanec a jeho přímý nadřízený
Kontrola:	vedoucí oddělení
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Všeobecné zásady ochrany informací firmy

Navrhované zásady ochrany informací při ukončení pracovního poměru

Při odchodu zaměstnance z firmy, navrhuji, aby:

- zaměstnanec předal veškerý software a hardware firmy

Odpovědnost:	zaměstnanec a regionální koordinátor infrastruktury IS
Kontrola:	vedoucí oddělení
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Ukončení pracovního poměru

- zaměstnanec předal dokumenty a další prostředky, které se k němu dostaly během jeho pracovního poměru,

Odpovědnost:	zaměstnanec a vedoucí oddělení
Kontrola:	vedoucí personálního oddělení
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Ukončení pracovního poměru

- veškerá přístupová práva ke všem informačním zdrojům udělená zaměstnanci byla při ukončení pracovního poměru neprodleně zrušena a to ke dni ukončení pracovní smlouvy,

[17] Dále použiji pojem **odpovědnost**, který představuje osobu odpovědnou za dodržování navrhovaných zásad.

Odpovědnost:	administrátor sítě
Kontrola:	regionální koordinátor infrastruktury IS
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Ukončení pracovního poměru

Bývalý zaměstnanec si nesmí ponechat žádnou kopii informací firmy.

3.1.2 Navrhovaná klasifikace informací

Navrhuji, aby všechny informace a dokumenty firmy byly zařazeny do jedné z následujících kategorií důvěrnosti v závislosti na jejich obsahu a důležitosti pro firmu. Poté budou zaměstnanci dostatečně informováni o tom, jak mohou s těmito informacemi nakládat. Každý zaměstnanec by měl být povinen dodržovat bezpečnostní opatření, odpovídající úrovni důvěrnosti svěřené informace nebo dokumentu.

Návrh úrovní důvěrnosti informací:

1. **Veřejné**

   Do této kategorie doporučuji zařadit informace, které jsou veřejně dostupné ze zdrojů, jako je internet, veřejný tisk, knihy a to jsou například:

   - prezentace výrobků,
   - marketingový materiál,
   - informace o firmě - její historie a vývoj, sídlo společnosti,
   - reference a doporučení od jiných firem,
   - hospodářské výsledky po veřejném publikování,
   - veřejné informace o vztazích firem,
   - počet zaměstnanců.

2. **Pro interní použití**

Na tuto úroveň navrhuji řadit informace, které se pohybují ve firmě a jejich zveřejnění firmu může poškodit. Jedná se například o:

- vnitřní sdělení,
- informace o projektech,
- nepublikované informace o produktech,
- seznamy klientů,
- detailní organizační struktura.

3. **Důvěrné**

Za důvěrné informace doporučuji považovat ty, které by v případě odhalení mohly vést k závažnému poškození společnosti. Toto odhalení může způsobit významnou finanční ztrátu, vést k porušení zákonů nebo předpisů, poškození klienta, ztrátu důvěry zákazníka, snížení provozní efektivity organizace a nebo dočasné ovlivnění image společnosti.

Do této kategorie navrhuji zařadit:

- taktické plány,
- vnitřní informace o trhu a konkurenci,
- smlouvy s prodejci a cenové nabídky,
- specifikace nových výrobků, které nejsou prozatím zveřejněny,
- informace týkající se řízení financí a účetnictví,
- osobní informace o zaměstnancích a bývalých zaměstnancích,
- přístupová hesla,
- informace ohledně informačního systému firmy, využívaných technologií (HW, SW), …

4. **Tajné**

Do této úrovně informací dle mého názoru patří majetkové informace, které v případě odhalení nějaké společnosti nebo jedinci kromě těch, které tyto informace specificky potřebují znát, mohou vést k podstatnému poškození společnosti, ovlivnit akciovou hodnotu společnosti, závažně porušit zákony či předpisy, poškodit strategického klienta, vést ke ztrátě image organizace, včetně ztráty pozice na trhu,

mít podstatný vliv na zisky, včetně ztráty klíčových pracovníků nebo pozastavení klíčových projektů.

Na tuto úroveň doporučuji zařadit:

- data o klientech,
- strategické plány společnosti,
- strategie budoucích výrobků a služeb,
- ochrana obchodní značky,
- kódovací klíče,
- detaily o bezpečnostních systémech a způsoby jejich zabezpečení.

Návrh postupu zacházení s dokumenty a informacemi:

Navrhovaný postup zacházení s firemními dokumenty a informacemi	1. Veřejné	2. Pro interní použití	3. Důvěrné	4. Tajné
DISTRIBUCE				
Pouze dle uvážení autora - žádné kopie				✓
Dle uvážení podle seznamu			✓	✓
Pouze pro interní použití - osobám, které je potřebují k práci		✓		
Dostupné pro veřejnost	✓			
ZPŮSOB DISTRIBUCE				
Papír	✓	✓	✓	✓
Přenosná elektronická média (CD, DVD, USB Flash, pásky a externí harddisky, ad.)	✓	✓	✓	✓
E-mailem	✓	✓	✗	✗
Šifrovaným e-mailem	✓	✓	✓	✓
Intranetem s kontrolou přístupu (ověření totožnosti a šifrovaný přenos)	✓	✓	✓	✗
Intranetem bez kontroly přístupu (bez ověření totožnosti)	✓	✓	✗	✗
Dostupné na internetové stránce firmy	✓		✗	✗
Uložení ve firemním PC	✓	✓	✓	✓
Uložení ve firemním PDA nebo v mobilním telefonu	✓	✓	✓	✗

Tabulka 4: Postup zacházení s informacemi a dokumenty dle klasifikace

Odpovědnost:	regionální koordinátor infrastruktury IS
Kontrola:	podnikový ředitel firmy
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Úrovně důvěrnosti informací a dokumentů a zacházení s nimi

3.1.3 Fyzická bezpečnost a bezpečnost prostředí

Návrh na fyzickou bezpečnost

Pro tuto oblast navrhuji, aby:

- každý, kdo se pohybuje v prostorách firmy, nosil viditelné označení totožnosti,
- byl přísný zákaz tailgatingu (současného projití dvou osob bezpečnostním koridorem na jednu identifikační kartu).

Odpovědnost:	zaměstnanec a bezpečnostní agentura
Kontrola:	personální oddělení
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Fyzická bezpečnost

Návrh přijímání návštěv do firmy

Pohyb cizích osob po firmě musí upravovat jistá pravidla, proto pro tuto část navrhuji, aby:

- všichni návštěvníci byli evidováni v návštěvní knize, musí se uvést přesná doba jejich příchodu a odchodu z firmy, podpis odpovědného pracovníka za tuto osobu, účel návštěvy,
- návštěva firmy nosila viditelné označení totožnosti (kartu s označením "návštěva firmy" s číselným označením, aby byla dohledatelná v knize návštěv),
- každá návštěva, která se pohybuje v oblastech s citlivými informacemi měla doprovod a schválení zodpovědnou osobou.

Odpovědnost:	bezpečnostní agentura a pracovník, kterého osoba/y navštěvují
Kontrola:	personální oddělení
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Návštěvy firmy

Návrh na zajištění bezpečnosti prostředí

Bezpečností prostředí je myšlena hlavně nepřítomnost zaměstnanců na svých pracovních místech, které při nedodržování těchto zásad může znamenat riziko, tudíž navrhuji, aby:

- každý zaměstnanec zajistil a přiměřeně ochránil zařízení firmy pokud je ponechává bez dozoru,
- každý dodržoval pravidlo „čistého stolu“: citlivé nebo důležité firemní informace a počítačové prostředky, které se nepoužívají musí být bezpečně uschovány a to při odchodu od stolu na dobu delší než 15 min.,
- přenosné počítače ponechal v prostorách firmy přiměřeně zabezpečeny,
- pro vytisknutí dokumentů z tiskáren používal osobní identifikační kartu, z toho důvodu, aby vytištěné dokumenty nebyly volně k dispozici jiným osobám,
- uživatelé, kteří dočasně odcházejí od PC aktivovali automatický software šetřiče obrazovky a zamkli nebo odhlásili svou pracovní stanici,
- uživatelé se řádně odhlásili ze všech systémů než na konci pracovní doby opustí pracoviště.

Odpovědnost:	zaměstnanec a jeho přímý nadřízený
Kontrola:	vedoucí oddělení
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Bezpečnost prostředí

3.1.4 Hardwarové a softwarové vybavení

Navrhované zásady pro užití hardwaru a softwaru firmy

V této oblasti počítačového vybavení doporučuji dodržovat následující zásady:

- použití informačních systémů, včetně HW a SW firmy pro jiné účely než firemní je přísně zakázáno, k povolení může dojít pouze v omezeném rozsahu, za všech okolností k tomu musí dát souhlas regionální koordinátor infrastruktury IS,
- zaměstnanci mohou používat pouze ta zařízení, která jsou pod kontrolou firmy,
- cizí zařízení nesmí být připojeno k firemní informační síti, což se týká i připojení pomocí dálkového přístupu, např. ze soukromého počítače doma,
- software musí být používán pouze dle jeho účelu,
- pro instalaci softwaru se musí dodržovat přísný postup,
- autorská práva a práva duševního vlastnictví firmy a třetích stran nesmějí být porušována,
- je možno používat pouze licencovaný a schválený software.

Odpovědnost:	zaměstnanec a jeho přímý nadřízený
Kontrola:	administrátor sítě
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Užívání hardwarového a softwarového vybavení

3.1.5 Kontrola přístupu k systému

Přístup k systému

Všechny přístupy k systému musí být zpětně dohledatelné, proto navrhuji, aby každý zaměstnanec:

- byl zodpovědný za všechny činnosti realizované pod svým osobním uživatelským přístupovým účtem,
- nesděloval svůj uživatelský účet nikomu jinému,
- nepoužíval cizí uživatelské účty.

Odpovědnost:	zaměstnanec
Kontrola:	administrátor sítě
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Přístup k systému

Správa hesel

Zaměstnanci musí dodržovat určitá pravidla při tvorbě hesel, proto navrhuji, aby každý pracovník:

- pravidelně měnil hesla uživatelských účtů a to i tehdy jestliže systém nevyžaduje změnu automaticky, standardní interval navrhuji na 60 dnů, u uživatelských účtů s vyššími přístupovými právy, to jsou účty vedoucích jednotlivých oddělení a úseků, managementu a ředitele firmy je nutné zvážit nastavení kratších intervalů, a zde doporučuji 30 dnů (interval je uživateli sdělen při jeho přijetí do pracovního poměru)

Pro tvorbu hesel navrhuji tato pravidla:

- minimální délka hesla 8 znaků, přičemž každé heslo musí obsahovat nejméně: jedno velké písmeno, jedno malé písmeno a jednu číslici,
- hesla nesmí být založena na žádných osobních informacích, aby někdo jiný nemohl snadno heslo odhadnout nebo odvodit na základě znalosti takovýchto informací, např. jména partnera a dětí, telefonních čísel, adresy, dat narození, atd.
- u ověřování totožnosti na základě uživatelských účtů uživatelé dostanou prvotní bezpečnostní heslo, které musí ihned po prvním přihlášení změnit.

Pro zacházení s hesly doporučuji tyto:

- hesla jsou klasifikována jako „důvěrné“; jsou osobními údaji a nikdy nesmějí být poskytovány dále,
- uživatelé jsou odpovědni za každý čin realizovaný pod jejich účtem,
- hesla se nesmí uchovávat na papíře nebo na některém z prostředků výpočetní techniky, pokud nejsou bezpečně uschována,

- hesla se nesmějí distribuovat nešifrovaným e-mailem,
- hesla se musí změnit vždy když jsou odhaleny, nebo pokud existuje nějaký náznak prozrazení,
- hesla nesmějí být zahrnuta do žádného automatického procesu přihlašování, např. nesmějí být použita v makru nebo jako funkční klávesa.
- pokud se počítač zeptá zda si má heslo zapamatovat pro příští použití, vždy musí zaměstnanec odpovědět „ne“.

Odpovědnost:	zaměstnanec a regionální koordinátor infrastruktury IS
Kontrola:	administrátor sítě
Dokument:	Směrnice o bezpečnosti informačních systémů – oblast: Správa hesel

3.1.6 Používání firemního e-mailu

Přístup na internet a přístup k poštovním systémům, který firma zajišťuje je nástroj pro zvýhodnění práce a na pomoc uživatelům při řešení firemních úkolů.
Pro tuto oblast navrhuji, aby:

- firma v souladu s platnými zákony a předpisy, rutinně monitorovala veškeré e-mailové a webové operace uživatelů pro účely plánování sítě, řízení toku a bezpečnosti dat,
- uživatelé neočekávali žádné soukromí pokud jde o informace přenášené nebo obdržené prostřednictvím internetu, intranetu a e-mailu, poskytovaných uživatelům firmou,
- firemní e-mail byl používán v souladu s místními správními statuty, předpisy a strategiemi a postupy firmy,
- je zakázáno používat firemní e-mail pro zasílání nebo uchovávání zpráv, které jsou znevažující, urážlivé, obscénní, obtěžující, výhružné vůči ostatním nebo podvodné.

3.1.7 Školení zaměstnanců

Doporučuji firmě, aby své zaměstnance z pohledu bezpečnostní politiky firmy řádně proškolila. Dle uvedených úrovní povědomí o bezpečnosti v analýze firmy z podkapitoly 1.3.8 navrhuji také odpovídající školení zaměstnanců zaměřené na právě zmiňované cílové skupiny zaměstnanců firmy.

Navrhuji, aby první dvě školení byla provedena externí firmou, další školení budou zajišťovat zaměstnanci z oddělení informačních systémů.

Dle současných ceníků specializujících se firem na bezpečnostní politiku v organizacích by mohlo školení firmu stát asi Kč 60 000,-. Tato cena zahrnuje dva dny na dodání služeb a dva dny na samotné školení zaměstnanců a to za předpokladu, že si odborné firmy účtují kolem Kč 15 000,- denně.

Firmě doporučuji, aby školení obnovovala a dále prohlubovala. Za zmínku stojí i informování zaměstnanců o různých bezpečnostních incidentech, které se kdekoli staly. Dle mého názoru je vždy konkrétní příklad dobrou ukázkou reality.

Z toho důvodu, aby se uživatelé firemního informačního systému mohli ke směrnicím bezpečnosti kdykoli vracet, navrhuji ji umístit na firemní intranet a ten neustále rozšiřovat o další informace. Doporučuji, aby správce systému zasílal nové informace, které řeší bezpečnost, do e-mailových schránek zaměstnanců např. jednou do měsíce nebo častěji dle potřeby.

3.2 Zálohování

3.2.1 Požadavky návrhu zálohování

Z pohledu co největšího zabezpečení dat ve firmě, navrhuji tyto požadavky pro nové zálohování:

1. Zálohovací médium musí být přenosné kvůli zajištění přenosu do trezoru ve firmě a odnesení zálohovaných dat do banky.
2. S rostoucími požadavky firmy se zálohování musí provádět na médium, které pojme větší objem dat. V současné době firma zálohu zhruba 380 GB denně,

proto navrhuji médium s kapacitou min. 800 GB. Na tom závisí výběr samotného zálohovacího zařízení. Z toho důvodu, že každoročně dojde ve firmě ke zhruba 10% nárůstu dat, se musí vzít v potaz fakt, že zařízení musí být použitelné i v budoucnu.

3. Přenosová rychlost musí být vyšší, aby zálohování všech dat proběhlo do jedné hodiny.
4. Podstatný pro samotné zálohování je zálohovací SW, který musí zvládnout zálohovat všechny tři servery.
5. Musí docházet k testování zálohovacích médií, aby byla potvrzena jejich funkčnost a jistota obnovy dat.

3.2.2 Návrh dvoustupňového zálohovacího systému

Moje navrhované řešení spočívá v metodě zálohování, která se nazývá Disk-To-Disk-To-Tape (D2D2T). Nejdříve se data zálohují na dostatečně velké diskové pole a následně jsou duplikována na páskovou knihovnu. Díky prvotní záloze na diskové pole jsou data nejen velmi rychle zálohována, ale především je možno je velmi rychle obnovit.

Výhod dvoustupňového zálohovacího systému je však celá řada. Mezi hlavní uvádím tyto:

- možnost paralelního zálohování několika serverů zároveň,
- možnost paralelního obnovy několika serverů zároveň,
- velice rychlá obnova dat (obnova z diskového prostoru začne probíhat okamžitě, data jsou okamžitě k dispozici),
- velice rychlé vytváření duplikátů dat z diskového prostoru na fyzické pásky (při vytváření duplikátů z disku na pásku jsou data na pásce již zapisována v souvislém formátu a to plnou rychlostí páskové mechaniky, což umožňuje rychlou obnov u i z páskového zařízení)
- pokročilý Media Management – na diskovém prostoru jsou uchovávána a tedy i na pásky přenášena pouze platná data,

- zajištění dat z pohledu Disaster Recovery (primární zálohovací diskové pole se umístí do jedné lokality a páskové knihovny s duplikovanými daty do druhé lokality, přičemž média po duplikaci lze odnášet do trezoru, tedy třetí lokality)
- ekonomický upgrade diskového pole.

3.2.3 Návrh zálohovacích mechanik a serveru

Pro řešení zálohovací mechaniky a serveru doporučuji použít hardware určený přímo pro tyto účely a od firmy Dell. Jak jsem již uvedla v analytické části, Dell bude v budoucnu firmy jedním globálním dodavatelem veškerého hardwarového vybavení. Specifikace tohoto zařízení viz Příloha 3 a 4.

Jedná se o řešení zálohování za Kč 387 000,-, které zahrnuje další komponenty včetně zálohovacího softwaru, HW a všech dalších potřebných služeb. Tato souhrnná cena je pouze orientační dle ceníku z internetu, firma může mít s firmou Dell vyjednané smluvní ceny za velký odběr hardwarových komponent.

3.2.4 Navrhovaná metoda a způsob zálohování

Z hlediska nejvyšší bezpečnosti dat, firmě doporučuji plné zálohování, které bude probíhat on-line. Pro uživatele informačního systému to nepředstavuje z hlediska množství zálohovaných dat problém ve velikosti zálohovacího okna. Zazálohování všech dat, která firma zálohovat potřebuje zabere zhruba jednu hodinu.

Navrhuji, aby firma zálohovala data denně na pevné disky a jednou týdně na pásky a pásky byly odneseny do banky, tak docílí dvojích bezpečně uložených záloh.

4 Zhodnocení a závěr

V této bakalářské práci jsem se snažila řešit problematiku bezpečnosti ve zvolené firmě, kde jsem na základě analýzy současného stavu informačního systému objevila největší problémy firmy.

Jednalo se především o nízké povědomí o bezpečnosti informačního systému u běžných uživatelů a jako druhý největší problém se vyskytlo zálohování dat, které nevyhovovalo současným potřebám firmy z hlediska množství zálohovaných dat.

Nejdůležitějším prvkem v první části návrhu řešení bylo dostatečné budování povědomí o bezpečnosti a bezpečnostní školení zaměstnanců, kde jsem stanovila pravidla bezpečnostní politiky firmy.

Veškeré směrnice a jiná nařízení nejsou efektivní, pokud nebudou dodržována a jejich porušení nebude postihováno, proto jsem tyto odpovědnosti v návrhové části práce určila. Také je velice důležité, aby pravidla a postupy ve firemních směrnicích pružně reagovala na nové technologie a současnou situaci potřeb bezpečnosti.

V druhé části návrhu řešení jsem firmě doporučila zálohování přes dvoustupňový zálohovací systém, který v poslední pár letech začíná být trendem pro zálohování dat ve firmách a zajišťuje vysokou bezpečnost uložených dat a jejich snadnou obnovu.

Problematika bezpečnosti informačních systémů je natolik komplexní téma, že není možné v rozsahu této práce její souhrnné pojednání ani v konkrétní firmě.

Seznam použité literatury

Knihy

[1] DOSEDĚL, T. *Počítačová ochrana a ochrana da*t. 1. vyd. Brno: Computer Press. 2004. 190 s. ISBN: 80-251-0106-1

[2] GÁLA, L., POUR, J. a TOMAN, P.. *Podniková informatika*. 1. vyd. Praha: Grada. 2006. 484 s. ISBN: 80-247-1278-4

[3] LEBER, J. *Windows NT. Zálohování a obnova dat*. 1. vyd. Praha: Computer Press. 1998. 282 s. ISBN: 80-7226-123-1

[4] RODRYČOVÁ, D. a STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy*. 1. vyd. Praha: Grada. 2002. 144 s. ISBN: 80-7169-144-5

[5] THOMAS, T. M. Zabezpečení *počítačových sítí bez předchozích znalostí*. 1. vyd. Brno: CP Books, 2005. 338 s. ISBN: 80-251-0417-6

[6] VITOVSKÝ, A. *Moderní slovník softwaru*. 1. vyd. Praha: AV Software. 2006. 588 s. ISBN 80-901428-8-5

Metodické příručky

[7] HANÁČEK, P. a STAUDEK, J. *Bezpečnost informačních systémů.* 1. vyd. Praha: Úřad pro státní informační systém. 2000. 128 s.
ISBN 80-238-5400-3

Firemní materiály

[8] *Disaster Recovery Plan Risk & Impact Analysis.* Kostelec nad Orlicí. 2005.

[9] *Information Systems Service Delivery - Global Infrastructure*. 2006

[10] OKUN, M.. *Disaster Recovery Plan - Global Repository.* 2003. 32 s.

[11] *Výroční zprávy firmy Federal-Mogulu, a. s. z let 2003 - 2005*. Kostelec nad Orlicí: Federal- Mogul, a. s. 2004 - 2006

Internetové adresy

[12] /online/ *Bezpečnost IS/ICT*. Dostupné z: http://www.aec.cz, převzato 16. 3. 2007

[13] /online/ *ČSN BS 7799-2:2004.* Dostupné z: http://www.micr.cz, převzato 11. 4. 2007

[14] /online/ http://www.dell.com

[15] /online/ *ISO 17799*. Dostupné z: http://www.iso.cz, převzato 30. 4. 2007

[16] /online/ KANTOR, R.. *Zálohování dat.* Dostupné z: http://www.fi.muni.cz, převzato 29. 10. 2006

[17] /online/ KATOLICKÝ, A. *Business Continuity Planning.* Dostupné z: http://www.akamonitor.cz/, převzato 25. 10. 2006

[18] /online/ MATOUŠ, R. *Možnosti zálohování databází obecně.* Dostupné z: http://www.trask.cz, převzato 17. 5. 2007

[19] /online/ NOVÁK, L. a ZAPLETALOVÁ, V. *Nová série bezpečnostních norem.* DSM. 2005. Dostupné z: http://www.dsm.tate.cz, převzato 3. 5. 2007

[20] /online/ *Příručka manažera III. – Business Continuity Planning.* Dostupné z: http://www.dsm.tate.cz/, převzato 5. 5. 2007

[21] /online/ *Záloha Disk-to-Disk-to-Tape.* Dostupné z: http://www.storage.cz, převzato 10. 5. 2007

[22] /online/ *Zálohování*. Dostupné z: http://www.storyflex.cz, převzato 19. 5. 2007

Seznam obrázků

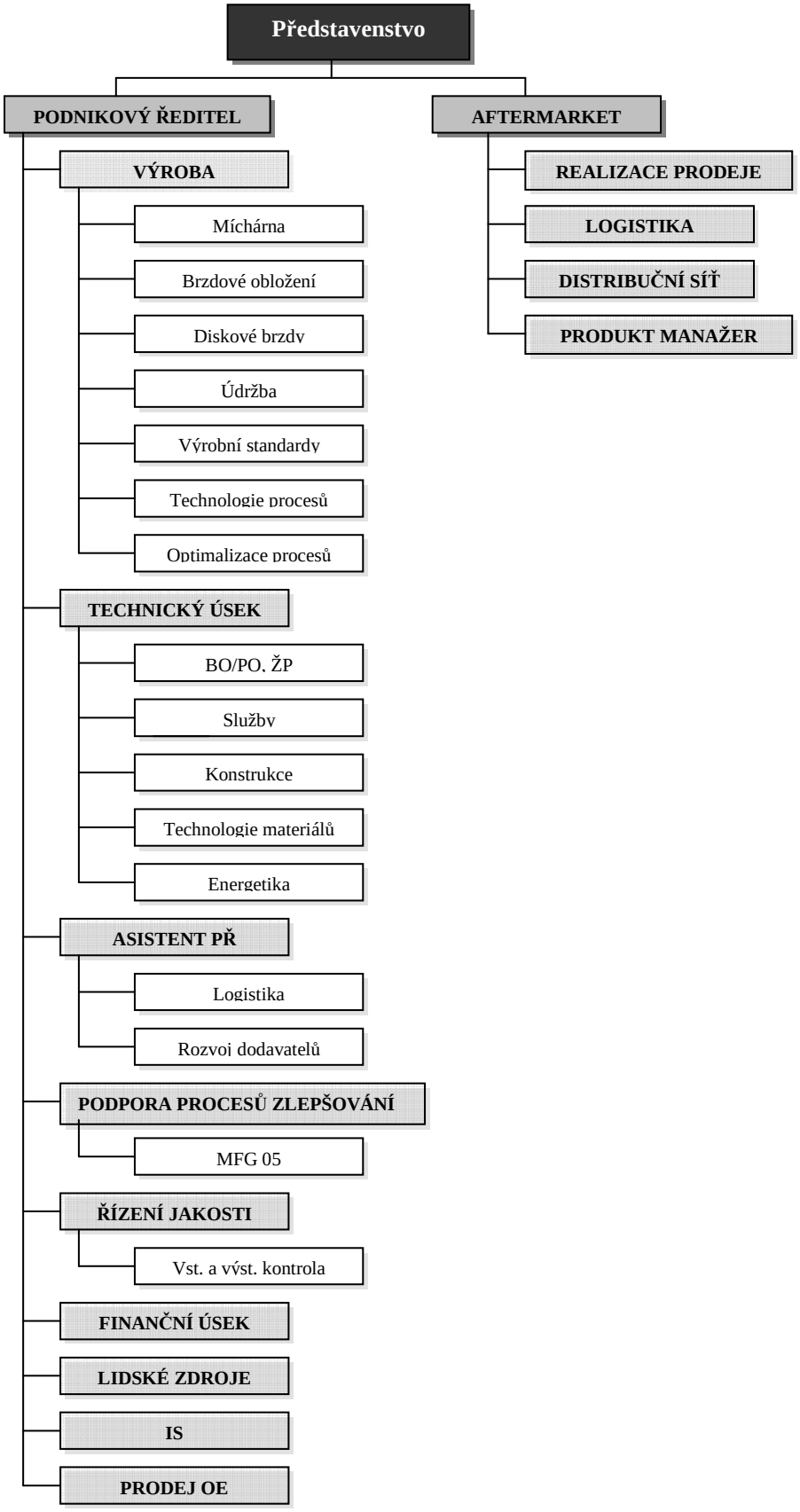
Seznam grafů

Seznam tabulek

Seznam příloh

Přílohy

Příloha 1: Organizační struktura společnosti



Příloha 2: Nejběžnější typy zásad zabezpečení

Název zásad	Popis
Přípustné šifrování	Stanovuje pravidla, která omezují šifrování jen na obecně známé, prověřené a účinné algoritmy. Navíc určuje potřebné postupy, které zajišťují naplnění příslušných zákonů a nižších předpisů.
Přípustné užití	Vymezuje osoby, které smí pracovat s počítačovým zařízením a sítěmi ve vlastnictví společnosti. Týká se firemních počítačů, umístěných ve firemních prostorách i v domácnostech zaměstnanců.
Analogové linky	Popisuje způsoby přípustného využívání analogových telefonních linek a linek ISDN a nařizuje příslušné zásady a postupy pro schvalování. Pro linky, určené výhradně k faxování a příjmu hovorů, a linky zapojené do počítačů platí samotná pravidla.
Poskytovatelé služeb	Vyjadřuje požadavky firmy na poskytovatele aplikačních služeb (Application Service Providers, ASP). Tito poskytovatelé zajišťují společně softwarové, hardwarové i síťové technologie. Součástí těchto zásad jsou také samostatné standardy poskytovatelů.
Standardy poskytovatelů aplikačních služeb	Definuje kritéria minimální bezpečnosti, kterou musí splňovat každý poskytovatel aplikačních služeb (ASP).
Audit	Členům oddělení informační bezpečnosti přiděluje oprávnění k výkonu bezpečnostního auditu nad libovolným systémem, který je ve vlastnictví společnosti nebo který je v jejich prostorách nainstalován.
Automaticky přeposílaná pošta	Zakazuje neoprávněné i neúmyslné prozrazování citlivých firemních informací.
Přístupové informace k databázím	Určuje požadavky na bezpečné ukládání a načítání uživatelských jmen a hesel k databázím (neboli přístupových informací), které budou využívat programy při přístupu k databázím provozované na firemní síti.
Vytáčený přístup	Stanovuje pravidla pro ochranu elektronických informací před neúmyslným ohrožením, jestliže oprávněný zaměstnanec pracuje nad vytáčeným připojením.
Extranet	Určuje zásady, podle nichž se do firemní sítě smí připojit cizí organizace za účelem provádění transakcí.
Citlivost informací	Napomáhá zaměstnancům určit, které informace smí sdělovat cizím osobám (mimo zaměstnanců), a také relativní citlivost informací, které se bez oprávnění sdělovat nesmí.
Bezpečnost vnitřních laboratoří	Definuje požadavky informační bezpečnosti v laboratořích, které zabraňují v ohrožení důvěrných informací a technologií, a také ochraňují provozní služby a ostatní zájmy firmy před pokusnými laboratorními aktivitami.
Antivirová ochrana	Vymezuje požadavky, jež musí splňovat všechny počítače

	připojené do podnikové sítě s ohledem na účinnou detekci virů a jejich prevenci.
Hesla	Zavádí standardy pro vytváření silných hesel, ochranu hesel a frekvenci změn hesel.
Vzdálený přístup	Definuje standardy pro připojení libovolného hostitele do firemní sítě. Tyto standardy sledují minimalizaci různých potenciálních hrozeb, jako je ztráta citlivých nebo důvěrných firemních dat, duševního vlastnictví, poškození image firmy na veřejnosti, poškození kriticky důležitých vnitřních systémů atd.
Posuzování rizik	Zmocňuje oddělení informační bezpečnosti k provádění pravidelného posuzování rizik bezpečnosti informací, jehož účelem je zjištění zranitelných míst v síti a zahájení nápravných opatření.
Zabezpečení směrovačů a přepínačů	Popisuje povinnou minimální bezpečnostní konfiguraci všech směšovačů a přepínačů, připojených do ostré provozní sítě, nebo používaných v jakémkoli ostrém provozním prostředí.
Zabezpečení serverů	Vymezuje standardy pro základní konfiguraci interních serverů, které jsou ve vlastnictví a/nebo provozu firmy, příp. které pracují ve webovém hostovaném prostoru.
Virtuální privátní síť (VPN)	Stanovuje zásady vzdáleného přístupu přes síť VPN s IPSec nebo L2TP do vnitřní firemní sítě.
Bezdrátová komunikace	Určuje pravidla pro přístup do podnikové sítě prostřednictvím zabezpečených mechanismů bezdrátové komunikace.

Zdroj: THOMAS, T. M. Zabezpečení *počítačových sítí bez předchozích znalostí.* 1. vyd. Brno: CP Books, 2005. s 56-57. ISBN: 80-251-0417-6

Příloha 3: Specifikace zálohovacího serveru

Dvouprocesorový Dell™ PowerEdge™ 2950, vybavený dvoujádrovými procesory Intel® Xeon™, přináší výkon nové generace kombinovaný s výbornou interní rozšiřitelností a hustotou racku. Představuje ideální volbu pro síťové aplikace jako je web, zprávy, databáze nebo konsolidace dat. Díky výborné konfigurační flexibilitě může PowerEdge 2950 nabídnout potřebný výkon i dostatečnou kapacitu disků pro stále rostoucí potřeby aplikací.

Podnikový výkon optimalizovaný pro rack a konfigurační flexibilita

Menší složitost - systém je konstruován pro ušetření času i nákladů při aktualizaci softwarových komponent jako je BIOS a ovladače. Vzhledová podobnost s PowerEdge 1950 a PowerEdge 2900 umožňuje uživatelům snížit náklady na správu několika platforem Dell. Společné hardwarové komponenty a jejich součinnost umožňují uplatnění jednotných postupů při správě a servisu, čímž zvyšují produktivitu administrátorů.

Konfigurační flexibilita - flexibilní šasi 2U nabízí dostatek prostoru pro budoucí růst a rozšíření, a přitom si zachovává skvělé rozměry ideální pro rack. Až šest 3,5" pevných disků nebo osm 2,5" pevných disků a mediální pozice pro páskovou mechaniku nabízejí dostatečnou flexibilitu pro potřeby různých aplikací.

Výkon a rozšiřitelnost - až dva dvoujádrové procesory Xeon a až 32 GB plně bufferované DIMM paměti umožňují aplikacím růst společně s podnikovými potřebami. TCP/IP Offload Engine (TOE) přispívá k lepší efektivitě sítě, zvlášť při práci s webovými aplikacemi nebo externím úložištěm iSCSI, neboť umožňuje hlavním systémovým procesorům soustředit se na samotné aplikace, a ne na datový proud.

Dell PowerEdge™ 2950 featuring Microsoft Windows Storage Server 2003 R2

SYSTÉMOVÉ KOMPONENTY

Dell PowerEdge™ 2950 featuring Microsoft Windows Storage Server 2003 R2

Dvoujádrový procesor Intel® Xeon® 5110, 4 MB vyrovnávací pamet, 1,60 GHz, 1066 MHZ FSB

Množství 1

Jednotka cena 136 000,00 Kč

Katalogové číslo:	**343419 PE2950WSS1**
Modul	**Popis**
Dell doporučuje	Dvoujádrový procesor Intel® Xeon® 5110, 4 MB vyrovnávací paměť, 1,60 GHz, 1066 MHZ FSB
Další procesor	Bez volby druhého procesoru
Paměť	2GB FB 667MHz Memory (2x1GB single rank DIMMs) - Energy Smart
Disketové mechaniky	No Floppy Disk Drive required
Síťové karty	Broadcom® NetXtreme 5721 Single Port Gigabit Ethernet NIC, Cu, PCIe x1
Optická mechanika	24X CD mechanika, interní, poloviční vý¿ka
Dokumentace k přepravě	PE2950 English rack power cord
1. pevný disk	300 GB 3,5palcový pevný disk SAS (10 000 ot./min.), pripojitelný za chodu
2. pevný disk	300 GB 3,5palcový pevný disk SAS (10 000 ot./min.), připojitelný za chodu
3. pevný disk	300 GB 3,5palcový pevný disk SAS (10 000 ot./min.), připojitelný za chodu
4. pevný disk	300 GB 3,5palcový pevný disk SAS (10 000 ot./min.), připojitelný za chodu
Instalační služby	No installation
Konektivita RAID	C3 - Integr. SAS / SATA, RAID 1, přídavný PERC 5/i radic, 2 pevné disky
Napájecí zdroj	One Non-Redundant Power Supply
Backplanes	1x4 propojovací deska pro 3,5palcové pevné disky
Kolejnice - rack	¿asi do racku s posuvnými kolejnicemi Rapid/Versa, univerzální
Informace o objednávce	PowerEdge Order - Czech Republic

Aktivace protokolu TCP/IP Offload Engine (TOE)	Broadcom TCP/IP Offload Engine Not Enabled
Riser karta	Riser s podporou PCI Express (2 PCIe x8 sloty; 1 PCIe x4 slot)
1. karta řadiče RAID nebo SCSI	PERC 5/i, základní deska x4, integrovaný RAID radic
Předistalovaný operační systém	Windows 2003 R2 Storage Server, Workgroup Edition (HW RAID) With Documentation - English
Další operační systém	Není zahrnuto
Systémová dokumentace	Serverový software OpenManage, s CD a dokumentací
Přední rám	Celní krytka pro PE2950

CELKEM::136 000,00 Kč

	Celkem bez DPH	Sazba DPH	Celkem včetně DPH
Mezisoučet	136 000,00 Kč	19,00%	**161 840,00 Kč**
Celková cena za doručení	1 800,00 Kč	19,00%	**2 142,00 Kč**
Celková cena	137 800,00 Kč	19,00%	**163 982,00 Kč**

Příloha 4: Specifikace zálohovací mechaniky

Dell PowerVault™ 114T

SYSTÉMOVÉ KOMPONENTY		
Dell PowerVault™ 114T	Množství	1
PV114T Single LTO3 Rack Base 2U, inc cleaning Cartridge	Jednotka cena	186 400,00 Kč

Katalogové číslo:	**343419 PV114T1**
Modul	**Popis**
Base	PV114T Single LTO3 Rack Base 2U, inc cleaning Cartridge
Dokumentace k přepravě	European - Documentation with PDU Cord
Standardní záruka	Base Warranty
Servisní balíčky	Upg to Standard Gold 3Y 4Hr Premier Enterprise Support (4Hr location only)
Instalační služby	Bez instalace
Kolejnice - rack	DELL 4 Post Rack Mount parts, all parts to fit a PV114T into a DELL Rack
Informace o objednávce	Power Vault Order - Czech Republic
Zálohovací software Symantec	Symantec Backup Exec 11d - Multi Server Suite
Yosemite Basic	No Yosemite Backup Software

CELKEM::186 400,00 Kč

	Celkem bez DPH	Sazba DPH	Celkem včetně DPH
Mezisoučet	186 400,00 Kč	19,00%	**221 816,00 Kč**
Celková cena za doručení	1 200,00 Kč	19,00%	**1 428,00 Kč**
Celková cena	187 600,00 Kč	19,00%	**223 244,00 Kč**